Rådet for
Den Europæiske Union

Bruxelles, den 26. november 2021
(OR. en)

14337/21

Interinstitutionel sag:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

NOTE

fra:	Generalsekretariatet for Rådet
til:	Rådet
Tidl. dok. nr.:	9583/2/21, 11724/21
Komm. dok. nr.:	14150/20
Vedr.:	Forslag til Europa-Parlamentets og Rådets direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 – *Generel indstilling*

I. INDLEDNING

1. Kommissionen vedtog den 16. december 2020 forslaget til direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (det reviderede NIS-direktiv eller "NIS 2")[1] med henblik på at erstatte det nuværende direktiv om sikkerhed for net- og informationssystemer ("NIS-direktivet")[2].

---

[1] Forslag til Europa-Parlamentets og Rådets direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148.

[2] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

Forslaget var et af de tiltag, der er fastsat i EU's strategi for cybersikkerhed for det digitale årti[3], med henblik på at sikre, at borgere og virksomheder drager fordel af pålidelige digitale teknologier.

2. Forslaget er baseret på artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF) og har til formål yderligere at forbedre offentlige og private enheders, kompetente myndigheders og Unionens samlede modstandsdygtighed og beredskabskapacitet.

3. I Europa-Parlamentet er Udvalget om Industri, Forskning og Energi (ITRE) ansvarligt for forslaget. ITRE-udvalget vedtog ordførerens betænkning den 28. oktober 2021.

4. Det Europæiske Økonomiske og Sociale Udvalg vedtog sin udtalelse den 28. april 2021.

5. Den 3. februar 2021 besluttede De Faste Repræsentanters Komité at høre Det Europæiske Regionsudvalg om forslaget[4]. Det Europæiske Regionsudvalg har endnu ikke afgivet udtalelse.

6. Den Europæiske Tilsynsførende for Databeskyttelse vedtog sin udtalelse den 11. marts 2021[5].

7. Rådet noterede sig i sine konklusioner[6] af 22. marts 2021 om EU's strategi for cybersikkerhed for det digitale årti det nye forslag, der bygger på NIS-direktivet, og gentog sin støtte til styrkelse og harmonisering af nationale rammer for cybersikkerhed og et vedvarende samarbejde mellem medlemsstaterne.

8. Det Europæiske Råd opfordrede i sine konklusioner den 21.-22. oktober 2021 til at fremme arbejdet med forslaget til et revideret NIS-direktiv.

---

[3] Dok. 14133/20.

[4] Dok. 5573/21.

[5] Udtalelse 5/2021 om cybersikkerhedsstrategien og NIS 2.0-direktivet.

[6] Dok. 6722/21.

II. ARBEJDET I RÅDETS FORBEREDENDE ORGANER

9. I Rådet er forslaget blevet behandlet af Den Horisontale Gruppe vedrørende Cyberspørgsmål (i det følgende benævnt "Cybergruppen"). Behandlingen af forslaget begyndte under det portugisiske formandskab den 19. januar med en nøje gennemgang af forslaget, hvor medlemsstaterne havde mulighed for at forelægge deres spørgsmål og fremhæve deres vigtigste betænkeligheder samt få detaljerede forklaringer fra Kommissionen om ændringerne i det reviderede direktiv.

10. Cybergruppen afsatte under det portugisiske formandskab 17 møder til præsentationen og gennemgangen af forslaget. En situationsrapport om gennemgangen blev forelagt på samlingen i TTE-Rådet den 4. juni 2021.

11. Arbejdet er siden fortsat og blevet intensiveret under det slovenske formandskab med henblik på at nå frem til en generel indstilling på samlingen i Rådet (transport, telekommunikation og energi) den 3. december 2021.Det slovenske formandskab har afsat 15 møder til revisionen af NIS 2-forslaget og mange bilaterale drøftelser på alle niveauer.

12. Cybergruppen fokuserede i første omgang sit arbejde på at omformulere forslagets tekst om samspillet mellem NIS 2-direktivet og sektorspecifik lovgivning og anvendelsesområdet, navnlig med hensyn til offentlig forvaltning, DNS-rodservere og udelukkelsesklausulen, og dernæst bl.a. på peerevalueringer, jurisdiktion og gensidig bistand, koordineret offentliggørelse af sårbarheder, databaser over domænenavne og registreringsdata og internationalt samarbejde.

13. Et første kompromisforslag om teksten til det foreslåede direktiv blev fremsat den 21. september 2021[7] på grundlag af skriftlige bemærkninger og uofficielle dokumenter fra medlemsstaterne samt de forudgående kompromisforslag om samspillet mellem NIS 2-direktivet og sektorlovgivningen og om anvendelsesområdet for NIS 2-direktivet.

---

[7] Dok. 12019/21.

14. Den seneste revision[8] af formandskabets kompromisforslag blev drøftet på gruppeniveau den 22. november 2021. Delegationerne hilste generelt kompromisteksten velkommen, men nogle få tog stadig undersøgelsesforbehold eller fremsatte bemærkninger til dele af kompromisforslaget. Der blev stadig foreslået en række tekniske omformuleringer i visse dele af teksten.

III. INDHOLD

15. På grundlag af drøftelserne på gruppeniveau er følgende punkter blevet peget på som de vigtigste politiske spørgsmål:

a) Anvendelsesområde (artikel 2)

Siden drøftelserne om NIS 2-forslaget blev indledt, har den største betænkelighed hos medlemsstaterne været den betydelige stigning i antallet af enheder, der er omfattet af direktivet, og navnlig indførelsen af størrelsesloftet, der indebærer, at alle mellemstore og store enheder, der opererer inden for de sektorer eller udbyder de tjenesteydelser, der er omfattet af NIS 2-direktivet, falder ind under dets anvendelsesområde. Selv om kompromisforslaget fastholder denne generelle regel, indeholder det yderligere bestemmelser for at sikre den nødvendige proportionalitet, et højere niveau af risikostyring og klare kriterier for så vidt angår den kritiske betydning med henblik på fastlæggelsen af de enheder, der er omfattet af direktivets anvendelsesområde. Kompromisforslaget indeholder desuden specifikke bestemmelser om prioritering af anvendelsen af tilsynsforanstaltninger efter en risikobaseret tilgang.

---

[8] Dok. 12019/5/21 REV 5.

b) Offentlig forvaltning (artikel 2, stk. 2a)

Medtagelsen af offentlige forvaltninger i anvendelsesområdet for NIS 2-direktivet var et meget debatteret emne, da sektoren for offentlig forvaltning er mere særskilt end de andre sektorer, der er omfattet af NIS 2-direktivet. Formandskabet har tilstræbt en afbalanceret tilgang, der tager hensyn til de særlige forhold, der gør sig gældende for de nationale rammer for offentlig forvaltning, og sikrer, at medlemsstaterne har en vis fleksibilitet, når det drejer sig om at afgøre, hvilke offentlige forvaltningsenheder der er omfattet af NIS 2. Derfor finder NIS 2 i kompromisteksten anvendelse på centralregeringers offentlige forvaltningsenheder, samtidig med at medlemsstaterne også kan fastsætte, at direktivet finder anvendelse på offentlige forvaltningsenheder på regionalt og lokalt niveau.

c) Udelukkelsesklausulen (artikel 2, stk. 3a og 3aa)

Medlemsstaterne ønskede at præcisere udelukkelsesklausulen yderligere, idet direktivet ikke finder anvendelse på enheder, der hovedsagelig udfører aktiviteter inden for områderne forsvar eller national sikkerhed eller aktiviteter, der vedrører national sikkerhed eller forsvar. Retsvæsenet, parlamenter, centralbanker er også udelukket.

d) Samspillet med sektorspecifik lovgivning

Medlemsstaterne understregede behovet for tilpasning mellem NIS 2-direktivet og sektorspecifik lovgivning, navnlig forordningen om digital operationel modstandsdygtighed i den finansielle sektor ("DORA"-forordningen) og direktivet om kritiske enheders modstandsdygtighed ("CER"-direktivet). NIS 2-direktivet, som bør være referencescenariet for minimumsharmonisering inden for cybersikkerhed, indeholder en særlig artikel om sektorspecifikke EU-retsakter (artikel 2b). Med hensyn til samspillet med CER-direktivet sikrer kompromisforslaget større klarhed vedrørende tilgangen, der omfatter alle risici. Andre vigtige tilføjelser vedrører samarbejdsordninger mellem de kompetente myndigheder i henhold til de respektive retsakter.

e) Peerlæring (artikel 16)

Med visse undtagelser var medlemsstaterne imod Kommissionens indførelse af obligatoriske peerevalueringer. Det foreslåede kompromis sikrer, at den nye peerlæringsmekanisme bygger på gensidig tillid og er en frivillig og medlemsstatsdrevet proces.

f) Jurisdiktion og territorialitet (artikel 24) og gensidig bistand (artikel 34)

Medlemsstaterne har udtrykt betænkeligheder ved konsekvenserne af at have en differentieret jurisdiktion for enheder i IKT-sektoren som foreslået af Kommissionen. Kompromisteksten har præciseret jurisdiktionen på grundlag af typen af enheder og styrket sproget om gensidig bistand.

g) Rapporteringsforpligtelser (artikel 20)

På baggrund af de betænkeligheder, som medlemsstaterne har givet udtryk for, og som vil overbebyrde enheder, der er omfattet af NIS 2-direktivet, og føre til overrapportering, er den obligatoriske rapportering for væsentlige cybertrusler udgået i kompromisteksten.

IV. KONKLUSION

16. De Faste Repræsentanters Komité nåede den 24. november 2021 til enighed om kompromisteksten i bilaget og besluttede at forelægge den for Rådet (transport, telekommunikation og energi) med henblik på vedtagelse af en generel indstilling.

17. Rådet opfordres derfor til at godkende den kompromistekst, som formandskabet har forelagt, jf. bilaget, og vedtage en generel indstilling på samlingen den 3. december 2021.

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV

om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[9],

under henvisning til udtalelse fra Regionsudvalget[10],

efter den almindelige lovgivningsprocedure, og

---

[9] EUT C af , s. .

[10] EUT C af , s. .

ud fra følgende betragtninger:

(1) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148[11] tog sigte på at opbygge cybersikkerhedskapaciteter i hele Unionen, afbøde trusler mod net- og informationssystemer, der anvendes til at levere væsentlige tjenester i nøglesektorer, og sikre kontinuiteten i sådanne tjenester, når de står over for cybersikkerhedshændelser, og dermed bidrage til Unionens økonomi og samfund, så de kan fungere effektivt.

(2) Siden ikrafttrædelsen af direktiv (EU) 2016/1148 er der gjort betydelige fremskridt med hensyn til at øge EU's modstandsdygtighed over for cybertrusler. Evalueringen af dette direktiv har vist, at det har fungeret som katalysator for den institutionelle og lovgivningsmæssige tilgang til cybersikkerhed i Unionen og har banet vejen for en betydelig holdningsændring. Direktivet har sikret færdiggørelsen af de nationale rammer ved at fastlægge nationale [...]strategier **for sikkerheden i net- og informationssystemer**, etablere nationale kapaciteter og gennemføre lovgivningsmæssige foranstaltninger, der omfatter væsentlige infrastrukturer og aktører, som hver medlemsstat har udpeget. Det har også bidraget til samarbejdet på EU-plan gennem oprettelsen af samarbejdsgruppen[12] og [...] netværk**et** af nationale enheder, der håndterer IT-sikkerhedshændelser ("CSIRT-netværket")[13]. Uanset disse resultater har evalueringen af direktiv (EU) 2016/1148 afsløret iboende mangler, der forhindrer det i effektivt at tackle aktuelle og nye cybersikkerhedsudfordringer.

---

[11] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

[12] Artikel 11 i direktiv (EU) 2016/1148.

[13] Artikel 12 i direktiv (EU) 2016/1148.

(3) Net- og informationssystemer har udviklet sig til et centralt element i hverdagen med den hurtige digitale omstilling og forbundethed i samfundet, herunder i forbindelse med grænseoverskridende udvekslinger. Denne udvikling har ført til en udvidelse af antallet og typen af trusler mod cybersikkerheden og skabt nye udfordringer, som kræver tilpassede, koordinerede og innovative svar i alle medlemsstater. Antallet, omfanget, den avancerede karakter, hyppigheden og virkningen af cybersikkerhedshændelser er stigende og udgør en alvorlig trussel mod net- og informationssystemernes funktion. Som følge heraf kan cyberhændelser hindre udøvelsen af økonomiske aktiviteter i det indre marked, medføre økonomiske tab, underminere brugernes tillid og forårsage store skader på Unionens økonomi og samfund. Cybersikkerhedsberedskab og -effektivitet er derfor mere afgørende for et velfungerende indre marked end nogensinde før.

(4) Retsgrundlaget for direktiv 1148/2016/EU var artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), hvis formål er det indre markeds oprettelse og funktion ved at styrke foranstaltninger til indbyrdes tilnærmelse af de nationale regler. De cybersikkerhedskrav, der pålægges enheder, som leverer tjenester eller økonomisk relevante aktiviteter, varierer betydeligt fra medlemsstat til medlemsstat med hensyn til typen af krav, detaljeringsgrad og tilsynsmetode. Disse forskelle medfører yderligere omkostninger og skaber vanskeligheder for virksomheder, der udbyder varer eller tjenesteydelser på tværs af grænserne. Krav, der stilles af en medlemsstat, og som er forskellige fra eller endog i konflikt med dem, der er pålagt af en anden medlemsstat, kan påvirke disse grænseoverskridende aktiviteter i væsentlig grad.

Desuden vil muligheden for en suboptimal udformning eller gennemførelse af cybersikkerheds[...]**foranstaltninger** i én medlemsstat sandsynligvis have konsekvenser for cybersikkerhedsniveauet i andre medlemsstater, navnlig i betragtning af de intense grænseoverskridende udvekslinger. Evalueringen af direktiv (EU) 2016/1148 har vist, at der er store forskelle i medlemsstaternes gennemførelse af det, herunder med hensyn til dets anvendelsesområde, hvis afgrænsning i vid udstrækning blev overladt til medlemsstaternes skøn. Direktiv (EU) 2016/1148 gav også medlemsstaterne meget vide skønsbeføjelser med hensyn til gennemførelsen af de sikkerheds- og hændelsesrapporteringsforpligtelser, der er fastsat deri. Disse forpligtelser blev derfor gennemført på vidt forskellige måder på nationalt plan. Lignende forskelle i gennemførelsen forekom i forhold til direktivets bestemmelser om tilsyn og håndhævelse.

(5) Alle disse forskelle medfører en fragmentering af det indre marked og kan have en negativ indvirkning på dets funktion og navnlig påvirke den grænseoverskridende levering af tjenester og cyberrobustheden som følge af anvendelsen af forskellige [...] **foranstaltninger**. Dette direktiv har til formål at fjerne sådanne store forskelle mellem medlemsstaterne, navnlig ved at fastsætte minimumsregler for, hvordan en koordineret reguleringsramme fungerer, ved at fastlægge mekanismer for effektivt samarbejde mellem de ansvarlige myndigheder i hver medlemsstat, ved at ajourføre listen over sektorer og aktiviteter, der er omfattet af cybersikkerhedsforpligtelser, og ved at tilvejebringe effektive retsmidler og sanktioner, der er afgørende for en effektiv håndhævelse af disse forpligtelser. Derfor bør direktiv (EU) 2016/1148 ophæves og erstattes af dette direktiv.

(6) [...]Medlemsstaterne **bør kunne** træffe de nødvendige foranstaltninger for at sikre beskyttelsen af sine væsentlige sikkerhedsinteresser, opretholde den offentlige orden og sikkerhed samt tillade efterforskning, afsløring og retsforfølgelse af strafbare handlinger[...]. [...]**Direktivet bør ikke finde anvendelse på visse offentlige eller private enherder, der udfører aktiviteter på disse områder. Den bør heller ikke finde anvendelse på aktiviteter, der udføres af enheder på disse områder. Desuden forpligtes** ingen medlemsstat til at meddele oplysninger, hvis udbredelse efter dens opfattelse ville stride mod dens væsentlige sikkerhedsinteresser. [...]**N**ationale regler [...] **eller** EU-regler om beskyttelse af fortrolige oplysninger, hemmeligholdelsesaftaler og uformelle hemmeligholdelsesaftaler, f.eks. Traffic Light Protocol[14], er af betydning.

(6a) EU-retten om beskyttelse af personoplysninger og privatlivets fred finder anvendelse på enhver behandling af personoplysninger i henhold til dette direktiv. Dette direktiv berører navnlig ikke forordning (EU) 2016/679 og Europa-Parlamentets og Rådets direktiv 2002/58/EF og bør derfor navnlig ikke berøre de opgaver og beføjelser, der tillægges de uafhængige tilsynsmyndigheder, som har kompetence til at overvåge overholdelsen af Unionens respektive databeskyttelseslovgivning.

---

[14] Traffic Light Protocol (TLP) giver en person, der deler oplysninger, mulighed for at informere sit publikum om eventuelle begrænsninger for videreformidlingen af disse oplysninger. Den anvendes i næsten alle CSIRT-fællesskaber samt visse informationsanalyse- og informationsdelingscentre (ISAC'er).

(7) Med ophævelsen af direktiv (EU) 2016/1148 bør anvendelsesområdet for de enkelte sektorer udvides til at omfatte en større del af økonomien i lyset af overvejelserne i betragtning 4-6. De sektorer, der er omfattet af direktiv (EU) 2016/1148, bør derfor udvides til at omfatte sektorer og tjenesteydelser af vital betydning for vigtige samfundsmæssige og økonomiske aktiviteter i det indre marked. Reglerne bør ikke være forskellige, alt efter om enhederne er operatører af væsentlige tjenester eller udbydere af digitale tjenester. Denne differentiering har vist sig at være forældet, da den ikke afspejler sektorernes eller tjenesteydelsernes reelle betydning for de samfundsmæssige og økonomiske aktiviteter i det indre marked.

(8) I overensstemmelse med direktiv (EU) 2016/1148 havde medlemsstaterne ansvaret for at afgøre, hvilke enheder der opfylder kriterierne for at blive betragtet som operatører af væsentlige tjenester ("identifikationsproces"). For at fjerne de store forskelle mellem medlemsstaterne i denne henseende og garantere retssikkerhed med hensyn til risikostyringskravene og rapporteringsforpligtelserne for alle relevante enheder bør der fastsættes et ensartet kriterium for, hvilke enheder der er omfattet af dette direktivs anvendelsesområde. Dette kriterium bør bestå i anvendelsen af reglen om størrelsesloftet, ifølge hvilken alle mellemstore og store virksomheder, som omhandlet i Kommissionens henstilling 2003/361/EF[15], som opererer inden for de sektorer eller leverer den type tjenester, der er omfattet af dette direktiv, er omfattet af direktivets anvendelsesområde. [...]

---

[15] Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

(8a) For at sikre et klart overblik over de enheder, der er omfattet af dette direktivs anvendelsesområde, bør medlemsstaterne kunne indføre nationale mekanismer for selvunderretning, der kræver, at enheder, der er omfattet af dette direktiv, som minimum fremsender deres navn, adresse og kontaktoplysninger samt den sektor, de opererer i, eller den type tjeneste, som de udbyder, og, hvor det er relevant, en liste over medlemsstater, hvor enheden udbyder sine tjenester til de kompetente myndigheder i henhold til dette direktiv, eller de organer, der er udpeget til dette formål af medlemsstaterne. Medlemsstaterne kan beslutte, hvad der er de egnede mekanismer, hvis der findes registre på nationalt plan, som gør det muligt at identificere de enheder, der er omfattet af dette direktivs anvendelsesområde.

(9) [...] **Mikroenheder eller** små [...] enheder, der opfylder visse kriterier, som indikerer, at de spiller en central rolle for medlemsstaternes økonomier eller samfund eller for bestemte sektorer eller typer af tjenesteydelser, bør dog også være omfattet af dette direktiv. Medlemsstaterne bør være ansvarlige for **som minimum** til Kommissionen at [...] **fremsende** [...] **de relevante oplysninger om antallet af identificerede enheder, den sektor, de tilhører, eller den type tjeneste, de udbyder, og de specifikke kriterier, som de er identificeret på grundlag af. Medlemsstaterne kan også, såfremt det er i overensstemmelse med de nationale sikkerhedsregler, beslutte at fremsende navnene på disse enheder til Kommissionen.**

(9a) Offentlige forvaltningsenheder, der udfører aktiviteter inden for områderne national sikkerhed, forsvar, offentlig sikkerhed, retshåndhævelse samt retsvæsen, parlamenter og centralbanker, er ikke omfattet af dette direktivs anvendelsesområde. I dette direktiv anses enheder med lovgivningskompetence ikke for at udføre aktiviteter inden for retshåndhævelse, og de er derfor med denne begrundelse ikke udelukket fra dette direktivs anvendelsesområde. Offentlige forvaltningsenheder, der er oprettet i fællesskab med et tredjeland i overensstemmelse med en international aftale, falder heller ikke ind under dette direktivs anvendelsesområde.

(9aa) Medlemsstaterne bør kunne fastslå, at enheder, der inden dette direktivs ikrafttræden er identificeret som operatører af væsentlige tjenester i overensstemmelse med direktiv (EU) 2016/1148, skal betragtes som væsentlige enheder.

(9aaa) Dette direktiv finder ikke anvendelse på medlemsstaternes diplomatiske og konsulære missioner i udlandet eller på deres IKT-infrastruktur, der anvendes af sådanne missioner, for så vidt en sådan infrastruktur befinder sig i udlandet eller drives for brugere i udlandet.

(10) Kommissionen kan i samarbejde med samarbejdsgruppen udstede retningslinjer for gennemførelsen af de kriterier, der gælder for mikrovirksomheder og små virksomheder.

(11) [...] **Enheder, der falder ind under dette direktivs anvendelsesområde, bør inddeles i to kategorier: væsentlige og vigtige, hvor der tages hensyn til sektorens og den udbudte tjenestetypes kritiske betydning samt deres størrelse. I den henseende bør der også tages behørigt hensyn til eventuelle relevante sektorspecifikke risikovurderinger eller vejledning fra de kompetente myndigheder, hvor det er relevant.** Både væsentlige og vigtige enheder bør være underlagt [...] risikostyringskrav og rapporteringsforpligtelser. Tilsyns- og sanktionsordningerne bør differentieres mellem disse to kategorier af enheder for at sikre en rimelig balance mellem **risikobaserede** krav og forpligtelser på den ene side og den administrative byrde, der følger af tilsynet med overholdelsen, på den anden side.

(12) **Dette direktiv fastsætter referencescenariet for foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser på tværs af alle sektorer, der er omfattet af dets anvendelsesområde. For at undgå fragmentering af cybersikkerhedsbestemmelserne i EU-retsakter bør Kommissionen, når det med henblik på at sikre et højt cybersikkerhedsniveau anses for nødvendigt med supplerende sektorspecifikke bestemmelser vedrørende** foranstaltninger til styring af cybersikkerhedsrisici **og rapporteringsforpligtelser vedrørende cybersikkerhed, vurdere, om sådanne bestemmelser kan fastsættes i en gennemførelsesretsakt i henhold til den beføjelse, der er fastsat i dette direktiv. Er sådanne retsakter ikke egnede til dette formål,** vil sektorspecifik lovgivning **kunne** bidrage til at sikre **et** højt [...] cybersikkerhedsniveau, samtidig med at der fuldt ud tages hensyn til [...] **de berørte** sektorers særlige og komplekse karakter. **Begrundelsen for, hvorfor en gennemførelsesretsakt i henhold til beføjelsen i dette direktiv ikke var hensigtsmæssig, skal forklares i den sektorspecifikke lovgivning. Samtidig bør sådanne sektorspecifikke bestemmelser i EU-retsakter tage behørigt hensyn til behovet for en omfattende og harmoniseret ramme for cybersikkerhed.** [...] Dette [...] berører ikke de eksisterende gennemførelsesbeføjelser, der er **tillagt** [...] Kommissionen inden for en række sektorer, herunder transport og energi.

(12a) Hvis en sektorspecifik EU-retsakt **indeholder bestemmelser, der** [...] kræver, at væsentlige eller vigtige enheder vedtager **foranstaltninger med en virkning, der mindst svarer til de forpligtelser, der er fastsat i dette direktiv, vedrørende** styring af cybersikkerhedsrisici [...] **og forpligtelser** til at underrette om **væsentlige** hændelser eller væsentlige cybertrusler [...], bør disse sektorspecifikke bestemmelser**, herunder om tilsyn og håndhævelse,** finde anvendelse. **Ved fastlæggelsen af, om virkningen svarer til de forpligtelser, der er fastsat i de sektorspecifikke bestemmelser i en EU-retsakt, bør følgende aspekter tages i betragtning: i) foranstaltningerne til styring af cybersikkerhedsrisici bør bestå af passende og forholdsmæssige tekniske og organisatoriske foranstaltninger til at styre risiciene for sikkerheden i net- og informationssystemer, som de relevante enheder anvender til at udbyde deres tjenester, og bør som minimum omfatte alle de elementer, der er fastsat i dette direktiv, ii) forpligtelsen til at underrette om væsentlige hændelser og cybertrusler bør mindst svare til de forpligtelser, der er fastsat i dette direktiv, for så vidt angår underretningernes indhold, format og tidsfrister, iii) enhedernes og de relevante myndigheders rapporteringsmetoder for sektorspecifikke EU-retsakter bør mindst svare til de krav, der er fastsat i dette direktiv, for så vidt angår deres indhold, format og tidsfrister og bør tage hensyn til CSIRT'ernes rolle, og iv) kravene vedrørende grænseoverskridende samarbejde for de relevante myndigheder bør mindst svare til de krav, der er fastsat i dette direktiv. Hvis de sektorspecifikke bestemmelser i en EU-retsakt ikke omfatter alle enheder i en specifik sektor, der falder ind under dette direktivs anvendelsesområde, bør de relevante bestemmelser i dette direktiv fortsat finde anvendelse på enheder, der ikke er omfattet af de pågældende sektorspecifikke bestemmelser.**

(12aa) Kommissionen **bør regelmæssigt evaluere anvendelsen af kravet om tilsvarende virkning i forbindelse med sektorspecifikke bestemmelser i EU-retsakter** [...]. **Kommissionen skal høre samarbejdsgruppen i forbindelse med forberedelsen af den regelmæssige evaluering**.

(12aaa) Fremtidige sektorspecifikke EU-retsakter bør tage behørigt hensyn til definitionerne i dette direktivs artikel 4 og de tilsyns- og håndhævelsesrammer, der er fastlagt i dette direktivs kapitel VI.

(12ab) Hvis sektorspecifikke bestemmelser i EU-retsakter kræver, at væsentlige eller vigtige enheder vedtager foranstaltninger med en virkning, der mindst svarer til de rapporteringsforpligtelser, der er fastsat i dette direktiv, bør overlappende rapporteringsforpligtelser undgås, og der bør sikres sammenhæng og effektivitet i håndteringen af underretninger om cybertrusler eller -hændelser. Med henblik herpå kan disse sektorspecifikke bestemmelser give medlemsstaterne mulighed for at oprette en fælles, automatisk og direkte rapporteringsmekanisme til underretning om væsentlige hændelser og cybertrusler til både de myndigheder, hvis opgaver er fastsat i de respektive sektorspecifikke bestemmelser, og de kompetente myndigheder, herunder alt efter omstændighederne det centrale kontaktpunkt og CSIRT'er, der er ansvarlige for de cybersikkerhedsopgaver, der er omhandlet i dette direktiv, eller en mekanisme, der sikrer en systematisk og øjeblikkelig udveksling af oplysninger og samarbejde mellem de relevante myndigheder og CSIRT'er vedrørende håndteringen af sådanne underretninger. Med henblik på at forenkle rapporteringen og gennemføre den fælles, automatiske og direkte rapporteringsmekanisme kan medlemsstaterne i overensstemmelse med sektorspecifik lovgivning anvende det fælles kontaktpunkt, som de opretter i henhold til dette direktivs artikel 11, stk. 5a. For at sikre harmonisering bør rapporteringsforpligtelserne i sektorspecifikke EU-retsakter tilpasses dem, der er fastsat i dette direktiv. Medlemsstaterne kan bestemme, at de kompetente myndigheder i henhold til dette direktiv eller de nationale CSIRT'er er adressater for rapporteringen i overensstemmelse med sektorspecifik lovgivning.

(13) Europa-Parlamentets og Rådets forordning XXXX/XXXX bør betragtes som en sektorspecifik EU-retsakt i forbindelse med dette direktiv for så vidt angår enheder i den finansielle sektor. Bestemmelserne i forordning XXXX/XXXX om risikostyringsforanstaltninger vedrørende informations- og kommunikationsteknologi (IKT), håndtering af IKT-relaterede hændelser og navnlig underretning om hændelser samt om afprøvning af digital operationel modstandsdygtighed, informationsdeling og IKT-tredjepartsrisiko bør finde anvendelse i stedet for bestemmelserne [...] **i** dette direktiv. Medlemsstaterne bør derfor ikke anvende bestemmelserne i dette direktiv om forpligtelser til risikostyring [...] og rapportering vedrørende cybersikkerhed samt tilsyn og håndhævelse på [...] finansielle enheder, der er omfattet af forordning XXXX/XXXX. Samtidig er det vigtigt at opretholde stærke forbindelser og udveksle oplysninger med den finansielle sektor i henhold til dette direktiv. Med henblik herpå giver forordning XXXX/XXXX [...] de europæiske tilsynsmyndigheder (ESA'er) for den finansielle sektor og de nationale kompetente myndigheder i henhold til forordning XXXX/XXXX[...] mulighed for at deltage i [...] **arbejdet** [...] i samarbejdsgruppen samt udveksle oplysninger og samarbejde med de centrale kontaktpunkter, der er udpeget i henhold til dette direktiv, [...] **samt** med de nationale CSIRT'er. De kompetente myndigheder i henhold til forordning XXXX/XXXX bør også fremsende oplysninger om større IKT-relaterede hændelser **og væsentlige cybertrusler** til de centrale kontaktpunkter**, de kompetente myndigheder eller de nationale CSIRT'er**, der er udpeget i henhold til dette direktiv. **Dette kan ske ved automatisk og direkte fremsendelse af hændelsesunderretninger eller via en fælles rapporteringsplatform.** Desuden bør medlemsstaterne fortsat medtage den finansielle sektor i deres cybersikkerhedsstrategier, og nationale CSIRT'er [...] **kan** dække den finansielle sektor i deres aktiviteter.

(13a) For at undgå huller mellem og overlapning af cybersikkerhedsforpligtelser, der pålægges enheder i luftfartssektoren, jf. punkt 2, litra a), i bilag I, bør de nationale myndigheder, der er udpeget i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008[16] og (EU) 2018/1139[17], og de kompetente myndigheder i henhold til dette direktiv samarbejde om gennemførelsen af foranstaltninger til styring af cybersikkerhedsrisici og tilsynet med disse foranstaltninger på nationalt plan. En enheds overholdelse af foranstaltningerne til styring af cybersikkerhedsrisici i henhold til dette direktiv kan af de nationale myndigheder, der er udpeget i henhold til forordning (EF) nr. 300/2008 og (EU) 2018/1139, anses for at være i overensstemmelse med kravene i disse og de relevante delegerede retsakter og gennemførelsesretsakter, der er vedtaget i henhold til nævnte forordninger.

---

[16] **Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed (security) inden for civil luftfart og om ophævelse af forordning (EF) nr. 2320/2002 (EUT L 97 af 9.4.2008, s. 72).**

[17] **Europa-Parlamentets og Rådets forordning (EU) 2018/1139 af 4. juli 2018 om fælles regler for civil luftfart og oprettelse af Den Europæiske Unions Luftfartssikkerhedsagentur og om ændring af forordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 og direktiv 2014/30/EU og 2014/53/EU og om ophævelse af forordning (EF) nr. 552/2004 og (EF) nr. 216/2008 og Rådets forordning (EØF) nr. 3922/91 (EUT L 212 af 22.8.2018, s. 1).**

(14) I betragtning af de indbyrdes forbindelser mellem cybersikkerhed og enheders fysiske sikkerhed bør der sikres en sammenhængende tilgang mellem Europa-Parlamentets og Rådets direktiv (EU) XXX/XXX og dette direktiv. Med henblik herpå bør medlemsstaterne sikre, at kritiske enheder **[**og tilsvarende enheder**]** i henhold til direktiv (EU) XXX/XXX betragtes [...] **som** væsentlige enheder i henhold til dette direktiv. Medlemsstaterne bør også sikre, at deres cybersikkerhedsstrategier skaber en politisk ramme for øget koordinering mellem den kompetente myndighed i henhold til dette direktiv og den kompetente myndighed i henhold til direktiv (EU) XXX/XXX i forbindelse med udveksling af oplysninger om hændelser og cybertrusler og udøvelse af tilsynsopgaver. **Kompetente** [...]**m**yndigheder i henhold til begge direktiver bør samarbejde og udveksle oplysninger, navnlig i forbindelse med identifikation af kritiske enheder, cybertrusler, cybersikkerhedsrisici, hændelser **samt om ikkecyberrelaterede risici, trusler og hændelser**, der påvirker kritiske enheder [eller **enheder, der svarer til kritiske enheder,]** [...] **herunder** cybersikkerhedsforanstaltninger **og fysiske** foranstaltninger, der træffes af kritiske enheder**, og resultaterne af tilsynsaktiviteter, der udføres med hensyn til sådanne enheder. For at strømline tilsynsaktiviteterne mellem de kompetente myndigheder, der er udpeget i henhold til begge direktiver, og for at mindske den administrative byrde mest muligt for de berørte enheder bør de kompetente myndigheder desuden bestræbe sig på at harmonisere modellerne til hændelsesunderretning og tilsynsprocesserne.** [...] **Hvis det er relevant, kan** kompetente myndigheder i henhold til direktiv (EU) XXX/XXX[...] **anmode** kompetente myndigheder i henhold til dette direktiv [...] om at udøve deres tilsyns- og håndhævelsesbeføjelser [...] **i forbindelse med** en væsentlig enhed, der er udpeget som kritisk. [...]

(14a) Enheder, der tilhører sektoren for digital infrastruktur, er i det væsentlige baseret på net- og informationssystemer, og derfor bør de forpligtelser, der pålægges disse enheder ved dette direktiv, på en omfattende måde omhandle sådanne systemers fysiske sikkerhed som led i deres forpligtelser til risikostyring og rapportering vedrørende cybersikkerhed. Da disse spørgsmål er omfattet af nærværende direktiv, finder forpligtelserne i kapitel III-VI i direktiv (EU) XXX/XXX [CER] ikke anvendelse på sådanne enheder.

(15) Opretholdelse og bevarelse af et pålideligt, modstandsdygtigt og sikkert domænenavnesystem (DNS) er en afgørende faktor for at bevare internettets integritet og er afgørende for dets fortsatte og stabile drift, som den digitale økonomi og det digitale samfund er afhængige af. Derfor bør dette direktiv finde anvendelse på udbydere af DNS-tjenester i DNS-**leverings- og** -oversættelseskæden, **som er af betydning for det indre marked,** herunder [...], topdomæne- (TLD-) navne**administratorer** [...], **enheder, der udbyder domænenavnsregistreringstjenester, operatører af** autoritative navneservere til domænenavne og **operatører af** rekursive resolvere. **Begrebet "DNS-tjenesteudbyder" bør ikke finde anvendelse på DNS-tjenester, der drives af den pågældende enhed og dens tilknyttede enheder til eget brug. De cybersikkerhedsforpligtelser, der følger af dette direktiv for denne kategori af udbydere, er strengt begrænset til foranstaltninger til styring og rapportering af cybersikkerhedsrisici og berører således ikke multiinteressentsamfundets styring af det globale DNS.**

(16) Cloudcomputingtjenester bør omfatte tjenester, der giver mulighed for on demand-adgang og bred fjernadgang til en skalerbar og elastisk pulje af delelige og distribuerede computerressourcer. Disse computerressourcer omfatter ressourcer såsom netværk, servere og anden infrastruktur, operativsystemer, software, lagring, applikationer og tjenester. **Tjenestemodellerne for cloudcomputing omfatter bl.a. infrastruktur som en service (IaaS), platform som en service (PaaS), software som en service (SaaS) og netværk som en service (NaaS).** Ibrugtagningsmodellerne for cloudcomputing bør omfatte privat, samfundsmæssig, offentlig og hybrid cloud. Ovennævnte tjeneste- og ibrugtagningsmodeller har samme betydning som de tjeneste- og ibrugtagningsmodeller, der er defineret i ISO/IEC 17788: 2014-standarden. Cloudcomputingbrugerens mulighed for ensidigt selvforsynende databehandlingskapacitet, såsom servertid eller netlagring, uden nogen menneskelig interaktion fra udbyderen af cloudcomputingtjenesters side, kan beskrives som on demand-administration. Udtrykket "bred fjernadgang" anvendes til at beskrive, at cloudkapaciteten leveres over nettet og tilgås gennem mekanismer, der fremmer brugen af heterogene tynde eller tykke klientplatforme (herunder mobiltelefoner, tablets, bærbare computere og arbejdsstationer).

Udtrykket "skalerbar" henviser til databehandlingsressourcer, der fordeles fleksibelt af udbyderen af cloudcomputingtjenester, uanset ressourcernes geografiske placering, med henblik på at håndtere udsving i efterspørgslen. Udtrykket "elastisk pulje" bruges til at beskrive de IT-ressourcer, der tilvejebringes og stilles til rådighed alt efter efterspørgslen for hurtigt at øge eller mindske de tilgængelige ressourcer alt efter arbejdsbyrden. Udtrykket "delbar" bruges til at beskrive de IT-ressourcer, der leveres til flere brugere, som deler en fælles adgang til tjenesten, men hvor databehandlingen foretages særskilt for hver bruger, selv om tjenesten leveres fra samme elektroniske udstyr. Udtrykket "distribueret" anvendes til at beskrive de databehandlingsressourcer, der befinder sig på forskellige netforbundne computere eller enheder, og som kommunikerer og koordinerer indbyrdes ved at sende meddelelser.

(17) I lyset af fremkomsten af innovative teknologier og nye forretningsmodeller forventes nye udrulnings- og tjenestemodeller for cloudcomputing at dukke op på markedet som reaktion på nye kundebehov. I denne forbindelse kan cloudcomputingtjenester leveres i en meget distribueret form, endnu tættere på de steder, hvor dataene genereres eller indsamles, hvorved man bevæger sig væk fra den traditionelle model og i retning af en meget distribueret model ("edge computing").

(18) Tjenester, der udbydes af datacentertjenesteudbydere, leveres ikke altid i form af cloudcomputingtjenester. Datacentre udgør derfor ikke altid en del af cloudcomputinginfrastrukturen. For at styre alle de risici, der er forbundet med sikkerheden i net- og informationssystemer, bør dette direktiv også omfatte udbydere af sådanne datacentertjenester, som ikke er cloudcomputingtjenester. I dette direktiv bør begrebet "datacentertjeneste" omfatte levering af en tjeneste, der omfatter strukturer eller grupper af strukturer, som er beregnet til central indkvartering, sammenkobling og drift af informationsteknologi og netværksudstyr, der leverer datalagrings-, behandlings- og transporttjenester, samt alle faciliteter og infrastrukturer til energidistribution og miljøkontrol. Begrebet "datacentertjeneste" finder ikke anvendelse på interne datacentre, der ejes og drives af den pågældende enhed til eget brug.

(19) Udbydere af posttjenester som omhandlet i Europa-Parlamentets og Rådets direktiv 97/67/EF[18] [...] **herunder** [...] udbydere af [...] kurertjenester**,** bør være omfattet af dette direktiv, hvis de leverer mindst ét led i postbefordringskæden og navnlig indsamling, sortering eller omdeling, herunder afhentning. Transporttjenester, der ikke udføres i forbindelse med et af disse trin, bør falde uden for posttjenesternes anvendelsesområde.

---

[18] Europa-Parlamentets og Rådets direktiv 97/67/EF af 15. december 1997 om fælles regler for udvikling af Fællesskabets indre marked for posttjenester og forbedring af disse tjenesters kvalitet (EFT L 15 af 21.1.1998, s. 14).

(20) Denne voksende indbyrdes afhængighed er resultatet af et stadig mere grænseoverskridende og indbyrdes afhængighedsskabende net af tjenester, der anvender centrale infrastrukturer i hele Unionen inden for sektorerne energi, transport, digital infrastruktur, drikkevand og spildevand, sundhed, visse aspekter af den offentlige forvaltning samt rummet, for så vidt som leveringen af visse tjenester, der er afhængige af jordbaserede infrastrukturer, som ejes, forvaltes og drives enten af medlemsstaterne eller af private parter, derfor ikke omfatter infrastruktur, der ejes, forvaltes eller drives af eller på vegne af Unionen som en del af dens rumprogrammer. Disse indbyrdes afhængighedsforhold betyder, at enhver afbrydelse, selv en, der oprindeligt var begrænset til én enhed eller én sektor, kan have kaskadevirkninger mere generelt, hvilket potentielt kan føre til vidtrækkende og langvarige negative virkninger for leveringen af tjenester i hele det indre marked. Covid-19-pandemien har vist, at vores stadig mere indbyrdes afhængige samfund er sårbare over for risici med lav sandsynlighed.

(20a) Med henblik på at opnå og opretholde et højt cybersikkerhedsniveau bør de nationale cybersikkerhedsstrategier, der kræves i henhold til dette direktiv, bestå af sammenhængende rammer, der sikrer en styring på cybersikkerhedsområdet. Disse strategier kan bestå af et eller flere dokumenter af lovgivningsmæssig eller ikkelovgivningsmæssig karakter.

(21) I betragtning af forskellene i de nationale forvaltningsstrukturer og for at beskytte allerede eksisterende sektorspecifikke ordninger eller Unionens tilsyns- og tilsynsorganer bør medlemsstaterne kunne udpege mere end én national kompetent myndighed, der er ansvarlig for at udføre de opgaver, som er forbundet med sikkerheden i væsentlige og vigtige enheders net- og informationssystemer i henhold til dette direktiv. Medlemsstaterne bør kunne tildele en eksisterende myndighed denne rolle.

(22) For at lette grænseoverskridende samarbejde og kommunikation mellem myndigheder og muliggøre en effektiv gennemførelse af dette direktiv er det nødvendigt, at hver medlemsstat udpeger et nationalt centralt kontaktpunkt med ansvar for koordinering af spørgsmål vedrørende sikkerheden i net- og informationssystemer og grænseoverskridende samarbejde på EU-plan.

(23) De kompetente myndigheder eller CSIRT'erne bør modtage underretninger om hændelser fra enheder på en effektiv måde**, også med henblik på, hvor det er relevant, at fremme en rettidig reaktion på hændelser og give den underrettende enhed et svar**. De centrale kontaktpunkter bør have til opgave at videresende underretninger om hændelser til de centrale kontaktpunkter i andre berørte medlemsstater. [...]

(23a) De sektorspecifikke EU-retsakter, der kræver foranstaltninger til styring af cybersikkerhedsrisici eller rapporteringsforpligtelser med en virkning, der mindst svarer til dem, der er fastsat i dette direktiv, kan fastsætte, at deres udpegede kompetente myndigheder udøver deres tilsyns- og håndhævelsesbeføjelser i forbindelse med sådanne foranstaltninger eller forpligtelser med bistand fra de kompetente myndigheder, der er udpeget i overensstemmelse med dette direktiv. De berørte kompetente myndigheder kan etablere samarbejdsordninger med henblik herpå. Sådanne samarbejdsordninger kan bl.a. præcisere procedurerne for koordinering af tilsynsaktiviteter, herunder procedurerne for undersøgelser og kontrol på stedet i overensstemmelse med national ret og en mekanisme for udveksling af relevante oplysninger mellem de kompetente myndigheder om tilsyn og håndhævelse, herunder adgang til cyberrelaterede oplysninger, som de kompetente myndigheder, der er udpeget i henhold til dette direktiv, anmoder om.

(24) Medlemsstaterne bør være udstyret med både tilstrækkelig teknisk og organisatorisk kapacitet til at forebygge, detektere, reagere på og afhjælpe hændelser og risici i net- og informationssystemer. Medlemsstaterne bør derfor sikre sig, at de har velfungerende CSIRT'er, også kendt som IT-beredskabsenheder ("CERT'er"), som opfylder de væsentlige krav med henblik for at sikre effektive og kompatible kapaciteter til at reagere på hændelser og risici og til sikre et effektivt samarbejde på EU-plan. Med henblik på at styrke tillidsforholdet mellem enhederne og CSIRT'erne [...] **kan** medlemsstaterne i tilfælde, hvor en CSIRT er en del af den kompetente myndighed, overveje en funktionel adskillelse mellem CSIRT'ernes operationelle opgaver, navnlig i forbindelse med udveksling af oplysninger og støtte til enhederne, og de kompetente myndigheders tilsynsaktiviteter.

(25) For så vidt angår personoplysninger bør CSIRT'er i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2016/679[19] for så vidt angår personoplysninger på vegne af og efter anmodning fra en enhed i henhold til dette direktiv være i stand til at foretage en proaktiv scanning af de net- og informationssystemer, der anvendes til levering af deres tjenester. Medlemsstaterne bør**, når det er relevant,** tilstræbe at sikre et ensartet niveau af teknisk kapacitet for alle sektorspecifikke CSIRT'er. Medlemsstaterne kan anmode Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) om bistand til at udvikle nationale CSIRT'er.

(26) I betragtning af betydningen af internationalt samarbejde om cybersikkerhed bør CSIRT'er kunne deltage i internationale samarbejdsnetværk i tillæg til de CSIRT-netværk, der er oprettet ved dette direktiv. **CSIRT'er og de kompetente myndigheder vil derfor kunne udveksle oplysninger, herunder personoplysninger, med tredjelandes CSIRT'er eller deres myndigheder med henblik på at udføre deres opgaver i overensstemmelse med forordning (EU) 2016/679. I tilfælde, hvor der ikke foreligger en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i overensstemmelse med artikel 45 i forordning (EU) 2016/679 eller passende garantier i henhold til artikel 46 i nævnte forordning, vil udvekslingen af personoplysninger, der anses for nødvendig med henblik på at afbøde væsentlige cybertrusler og reagere på en igangværende væsentlig hændelse, kunne anses for at udgøre en vigtig samfundsinteresse som omhandlet i artikel 49, stk. 1, litra d), i forordning (EU) 2016/679.**

---

[19] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

(27) I overensstemmelse med bilaget til Kommissionens henstilling (EU) 2017/1548 om koordineret reaktion på store cybersikkerhedshændelser og -kriser ("planen")[20] skal en væsentlig hændelse forstås som en hændelse med en betydelig indvirkning på mindst to medlemsstater, eller hvis forstyrrende virkninger overstiger en medlemsstats kapacitet til at reagere på den. Alt efter årsag og virkning kan omfattende hændelser eskalere og udvikle sig til fuldgyldige kriser, der forhindrer det indre markeds korrekte funktion. I betragtning af sådanne begivenheders vidtrækkende omfang og i de fleste tilfælde grænseoverskridende karakter bør medlemsstaterne og relevante EU-institutioner, -organer og -agenturer samarbejde på teknisk, operationelt og politisk plan for at koordinere indsatsen i hele Unionen.

(28) Eftersom udnyttelsen af sårbarheder i net- og informationssystemer kan forårsage betydelige forstyrrelser og skader, er hurtig identifikation og afhjælpning af disse sårbarheder en vigtig faktor med hensyn til at reducere cybersikkerhedsrisikoen. Enheder, der udvikler **eller administrerer** sådanne systemer, bør derfor indføre passende procedurer til håndtering af sårbarheder, når de opdages. Da sårbarheder ofte opdages og indberettes (afsløres) af tredjeparter (underrettende enheder), bør producenten eller udbyderen af IKT-produkter eller -tjenester også indføre de nødvendige procedurer for modtagelse af sårbarhedsoplysninger fra tredjeparter. I denne forbindelse indeholder de internationale standarder ISO/IEC 30111 og ISO/IEC [...] **29147** vejledning om henholdsvis håndtering af sårbarheder og offentliggørelse af sårbarheder. Hvad angår oplysninger om sårbarheder er koordinering mellem de underrettende enheder og producenter eller udbydere af IKT-produkter eller -tjenester særlig vigtig. Koordineret offentliggørelse af sårbarheder angiver en struktureret proces, hvorigennem sårbarheder indberettes til organisationer på en måde, der gør det muligt for organisationen at diagnosticere og afhjælpe sårbarheden, inden detaljerede sårbarhedsoplysninger videregives til tredjeparter eller offentligheden. Koordineret offentliggørelse af sårbarheder bør også omfatte koordinering mellem den underrettende enhed og organisationen med hensyn til tidspunktet for afhjælpning og offentliggørelse af sårbarheder.

---

[20] Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

(29) Medlemsstaterne bør derfor træffe foranstaltninger til at fremme koordineret offentliggørelse af sårbarheder ved at fastlægge en relevant national politik. **Som led i deres nationale politik bør medlemsstaterne så vidt muligt tackle de udfordringer, som sårbarhedsforskere står over for, herunder deres potentielle strafansvar, i overensstemmelse med deres nationale retsorden.** [...]Medlemsstaterne bør udpege en CSIRT til at påtage sig rollen som "koordinator", der fungerer som formidler mellem de underrettende enheder og producenter eller udbydere af IKT-produkter eller -tjenester, hvor det er nødvendigt. CSIRT-koordinatorens opgaver bør navnlig omfatte identifikation af og kontakt til berørte enheder, støtte til underrettende enheder, forhandling af tidsfrister for offentliggørelse og håndtering af sårbarheder, der påvirker flere organisationer (**koordineret** offentliggørelse af sårbarheder med flere parter). Hvis **den rapporterede** sårbarhed **potentielt vil kunne have væsentlig indvirkning på enheder** [...] i mere end én medlemsstat, bør de udpegede CSIRT'er [...] samarbejde inden for CSIRT-netværket**, hvis det er relevant**.

(30) Adgang til korrekte og rettidige oplysninger om sårbarheder, der påvirker IKT-produkter og -tjenester, bidrager til en forbedret risikostyring i forbindelse med cybersikkerhed. I denne henseende er kilder til offentligt tilgængelige oplysninger om sårbarheder et vigtigt redskab for enheder og deres brugere, men også for nationale kompetente myndigheder og CSIRT'er. Derfor bør ENISA oprette et sårbarhedsregister, hvor væsentlige og vigtige enheder og deres leverandører samt enheder, der ikke er omfattet af dette direktivs **eller udpegede CSIRT'ers** anvendelsesområde, på frivillig basis kan afsløre sårbarheder og fremlægge de sårbarhedsoplysninger, der gør det muligt for brugerne at træffe passende afbødende foranstaltninger.

(31) Selv om der findes lignende sårbarhedsregistre eller -databaser, hostes og vedligeholdes disse af enheder, der ikke er etableret i Unionen. Et europæisk sårbarhedsregister, der føres af ENISA, vil give større gennemsigtighed med hensyn til offentliggørelsesprocessen, inden sårbarheden offentliggøres officielt, og modstandsdygtighed i tilfælde af forstyrrelser eller afbrydelser af leveringen af tilsvarende tjenester. For at undgå dobbeltarbejde og tilstræbe komplementaritet i videst muligt omfang bør ENISA undersøge muligheden for at indgå strukturerede samarbejdsaftaler med lignende registre i tredjelandes jurisdiktioner. **ENISA bør navnlig undersøge muligheden for et tæt samarbejde med operatørerne af Common Vulnerabilities and Exposures (CVE) system, herunder muligheden for at blive en root CVE numbering authority.**

(32) **Samarbejdsgruppen bør fortsat støtte og lette det strategiske samarbejde og udvekslingen af oplysninger samt styrke tilliden og fortroligheden blandt medlemsstaterne.** Samarbejdsgruppen bør hvert andet år udarbejde et arbejdsprogram, der omfatter de foranstaltninger, som gruppen skal gennemføre for at nå sine mål og udføre sine opgaver. Tidsrammen for det første program, der vedtages i henhold til dette direktiv, bør tilpasses tidsrammen for det sidste program, der er vedtaget i henhold til direktiv (EU) 2016/1148, for at undgå potentielle afbrydelser af gruppens arbejde.

(33) Samarbejdsgruppen bør i forbindelse med udarbejdelse af vejledningsdokumenter kortlægge nationale løsninger og erfaringer, vurdere virkningen af samarbejdsgruppens resultater på nationale tilgange, drøfte gennemførelsesudfordringer og formulere specifikke anbefalinger, der skal tackles gennem bedre gennemførelse af eksisterende regler.

(34) Samarbejdsgruppen bør fortsat være et fleksibelt forum og være i stand til at reagere på skiftende og nye politiske prioriteter og udfordringer, samtidig med at der tages hensyn til de disponible ressourcer. Den bør tilrettelægge regelmæssige fælles møder med relevante private interessenter fra hele Unionen for at drøfte gruppens aktiviteter og indsamle input om nye politiske udfordringer. For at styrke samarbejdet på EU-plan bør gruppen overveje at indbyde de EU-organer og -agenturer, der er involveret i cybersikkerhedspolitikken, såsom Det Europæiske Center til Bekæmpelse af IT-Kriminalitet (EC3), Den Europæiske Unions Luftfartssikkerhedsagentur (EASA) og Den Europæiske Unions Agentur for Rumprogrammet (EUSPA), til at deltage i dets arbejde.

(35) De kompetente myndigheder og CSIRT'er bør have beføjelse til at deltage i udvekslingsordninger for embedsmænd fra andre medlemsstater for at forbedre samarbejdet. De kompetente myndigheder bør træffe de foranstaltninger, der er nødvendige for at sætte embedsmænd fra andre medlemsstater i stand til at spille en effektiv rolle i den kompetente myndigheds aktiviteter.

(35a) CSIRT-netværket bør fortsat bidrage til at styrke fortroligheden og tilliden og fremme et hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne. For at styrke det operationelle samarbejde på EU-plan bør CSIRT-netværket overveje at indbyde de EU-organer og -agenturer, der er involveret i cybersikkerhedspolitikken, såsom Europol, til at deltage i sit arbejde.

(36) [...]

(36a) For at lette en effektiv gennemførelse af bestemmelserne i dette direktiv, herunder vedrørende håndtering af sårbarheder, styring af cybersikkerhedsrisici, rapporteringsforanstaltninger og informationsudvekslingsordninger, kan medlemsstaterne samarbejde med tredjelande og gennemføre aktiviteter, der anses for hensigtsmæssige til dette formål, herunder udveksling af oplysninger om trusler, hændelser, sårbarheder, værktøjer og metoder, taktikker, teknikker og procedurer, beredskab og øvelser i forbindelse med cyberkrisestyring, uddannelse, tillidsskabende foranstaltninger og strukturerede informationsudvekslingsordninger. Sådanne samarbejdsaftaler bør være i overensstemmelse med EU-retten om databeskyttelse.

(37) Medlemsstaterne bør bidrage til oprettelsen af EU's krisereaktionsramme for cybersikkerhed som fastsat i henstilling (EU) 2017/1584 gennem de eksisterende samarbejdsnetværk, navnlig Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser (EU-CyCLONe), CSIRT-netværket og samarbejdsgruppen. EU-CyCLONe og CSIRT-netværket bør samarbejde på grundlag af proceduremæssige ordninger, der fastlægger de nærmere bestemmelser for dette samarbejde, **og undgå dobbeltarbejde**. EU-CyCLONe's forretningsorden bør yderligere præcisere, hvordan netværket skal fungere, herunder, men ikke begrænset til, roller, samarbejdsmetoder, interaktion med andre relevante aktører og modeller for informationsudveksling samt kommunikationsmidler. Med hensyn til krisestyring på **politisk** EU-plan bør de relevante parter være afhængige af de integrerede ordninger for politisk kriserespons (IPCR). Kommissionen bør anvende den tværsektorielle krisekoordinationsproces på højt niveau i ARGUS til dette formål. Hvis krisen har en vigtig ekstern dimension eller berører den fælles sikkerheds- og forsvarspolitik (FSFP), bør EU-Udenrigstjenestens krisereaktionsmekanisme (CRM) aktiveres.

(37a) **EU-CyCLONe bør fungere som et netværk mellem det tekniske og politiske niveau under store cybersikkerhedshændelser og -kriser. Det bør styrke samarbejdet på operationelt plan ved at bygge på CSIRT-netværkets resultater og bruge egne kapaciteter til at udarbejde konsekvensanalyser af omfattende hændelser og kriser og støtte beslutningstagningen på politisk plan. EU-institutionerne, -organerne og -agenturerne bør udpege en kompetent myndighed med ansvar for håndtering af omfattende sikkerhedshændelser og -kriser til medlem af EU-CyCLONe.**

(38) [...]

(39) [...]

(39a) **Ansvaret for at sikre sikkerheden i net- og informationssystemer ligger i vid udstrækning hos væsentlige og vigtige enheder. En risikostyringskultur med risikovurdering og gennemførelse af sikkerhedsforanstaltninger, som står i forhold til risiciene, bør fremmes og udvikles.**

(40) Risikostyringsforanstaltninger bør **tage hensyn til enhedens grad af afhængighed af net- og informationssystemer og** omfatte foranstaltninger til at identificere alle risici for hændelser, forebygge, opdage og håndtere hændelser og begrænse deres konsekvenser. Sikkerheden i net- og informationssystemer bør omfatte sikkerheden for lagrede, overførte og behandlede data.

(40a) Da trusler mod net- og informationssystemers sikkerhed kan have forskellig oprindelse, anvender dette direktiv en tilgang, der omfatter alle risici, som inkluderer beskyttelse af net- og informationssystemer og deres fysiske miljø mod enhver begivenhed, som f.eks. tyveri, brand, oversvømmelse, telekommunikations- eller strømsvigt, eller mod uautoriseret fysisk adgang og skade på eller indgreb i enhedens informationer og informationsbehandlingsfaciliteter, som kan bringe tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare. Risikostyringsforanstaltningerne bør derfor også tage hånd om den fysiske og miljømæssige sikkerhed ved at inkludere foranstaltninger til beskyttelse af enhedens net- og informationssystemer mod systemsvigt, menneskelige fejl, ondsindede handlinger eller naturfænomener i overensstemmelse med europæiske eller internationalt anerkendte standarder, såsom dem, der er omfattet af ISO 27000-serien. I den forbindelse bør enhederne som led i deres risikostyringsforanstaltninger også tage hånd om personalesikkerheden og indføre passende adgangskontrolpolitikker. Disse foranstaltninger bør hænge sammen med direktiv XXXX [CER-direktivet].

(40b) I mangel af passende europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i overensstemmelse med forordning (EU) 2019/881, kan medlemsstaterne kræve, at enheder anvender certificerede IKT-produkter, -tjenester og -processer eller indhenter en attest i henhold til tilgængelige nationale cybersikkerhedsordninger med henblik på at opfylde kravene til styring af cybersikkerhedsrisici i henhold til dette direktiv.

(41) Med henblik på at undgå at operatører af væsentlige og vigtige enheder pålægges en uforholdsmæssig stor økonomisk og administrativ byrde, bør kravene til styring af cybersikkerhedsrisici stå i et rimeligt forhold til risikoen [...] **for** det pågældende net- og informationssystem under hensyntagen til sådanne foranstaltningers aktuelle tekniske niveau **og implementeringsomkostninger.**. **Der bør også tages behørigt hensyn til enhedens størrelse samt sandsynligheden for, at der indtræffer hændelser, og til hvor alvorlige de er.**

(41a) Med henblik på at lette de reguleringsmæssige byrder bør kravene til gennemførelsen af foranstaltninger til styring af cybersikkerhedsrisici for små og mellemstore enheder eller mikroenheder i princippet være lempeligere, medmindre kriterier vedrørende kritisk betydning eller nationale risikovurderinger ville berettige til strengere krav, navnlig med hensyn til enheder, der opfylder de kriterier vedrørende kritisk betydning, der er fastsat i dette direktiv.

(42) Væsentlige og vigtige enheder bør garantere sikkerheden i de net- og informationssystemer, som de anvender i forbindelse med deres aktiviteter. Der er primært tale om private net- og informationssystemer, der forvaltes af deres interne IT-personale, eller hvis sikkerhed er blevet outsourcet. Kravene til risikostyring og rapportering vedrørende cybersikkerhed i henhold til dette direktiv bør finde anvendelse på de relevante væsentlige og vigtige enheder, uanset om de udfører vedligeholdelsen af deres net- og informationssystemer internt eller outsourcer den.

(42aa) Under hensyntagen til deres grænseoverskridende karakter bør DNS-tjenesteudbydere, topdomænenavneadministratorer og enheder, der udbyder domænenavnregistreringstjenester til topdomæner, udbydere af cloudcomputingtjenester, udbydere af datacentertjenester og udbydere af indholdsleveringsnetværk, udbydere af administrerede tjenester og udbydere af administrerede sikkerhedstjenester være omfattet af en højere grad af harmonisering på EU-plan. Gennemførelsen af cybersikkerhedsforanstaltninger bør derfor muliggøres ved hjælp af en gennemførelsesretsakt.

(43) Håndtering af cybersikkerhedsrisici, der stammer fra en enheds forsyningskæde og dens forhold til sine leverandører, er særlig vigtig i betragtning af udbredelsen af hændelser, hvor enheder er blevet ofre for cyberangreb, og hvor ondsindede aktører har været i stand til at bringe sikkerheden i en enheds net- og informationssystemer i fare ved at udnytte sårbarheder, der påvirker tredjepartsprodukter og -tjenester. Enheder bør derfor vurdere og tage hensyn til den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer.

(44) Blandt tjenesteudbydere spiller udbydere af administrerede sikkerhedstjenester (MSSP'er) på områder som reaktion på hændelser, penetrationstest, sikkerhedsrevisioner og konsulentbistand en særlig vigtig rolle med hensyn til at bistå enheder i deres bestræbelser på at opdage og reagere på hændelser. Disse MSSP'er har imidlertid også selv været mål for cyberangreb og udgør i kraft af deres tætte integration i operatørernes aktiviteter en særlig cybersikkerhedsrisiko. Enheder bør derfor udvise øget omhu ved udvælgelsen af en MSSP.

(44a) De nationale kompetente myndigheder kan i forbindelse med deres tilsynsopgaver også drage fordel af cybersikkerhedstjenester såsom sikkerhedsrevisioner og penetrationstest eller reaktion på hændelser. For at bistå enheder samt nationale kompetente myndigheder med at udvælge kvalificerede og pålidelige udbydere af cybersikkerhedstjenester bør Kommissionen med bistand fra samarbejdsgruppen og ENISA overveje muligheden for at anmode om europæiske cybersikkerhedscertificeringsordninger i overensstemmelse med artikel 48 i forordning (EU) 2019/881.

(45) Enheder bør også tage højde for cybersikkerhedsrisici, der stammer fra deres samspil og forbindelser med andre interessenter inden for et bredere økosystem. Navnlig bør enheder træffe passende foranstaltninger til at sikre, at deres samarbejde med akademiske institutioner og forskningsinstitutioner finder sted i overensstemmelse med deres cybersikkerhedspolitikker og følger god praksis med hensyn til sikker adgang til og formidling af oplysninger generelt og beskyttelse af intellektuel ejendom i særdeleshed. På samme måde bør enhederne i betragtning af dataenes betydning og værdi for enhedernes aktiviteter, træffe alle passende cybersikkerhedsforanstaltninger, når de benytter sig af datatransformations- og dataanalysetjenester fra tredjeparter.

(46) For yderligere at håndtere centrale risici i forsyningskæden og bistå enheder, der opererer i sektorer, som er omfattet af dette direktiv, med at håndtere cybersikkerhedsrisici i forsyningskæden og vedrørende leverandører hensigtsmæssigt, bør samarbejdsgruppen, der involverer relevante nationale myndigheder, i samarbejde med Kommissionen og ENISA foretage koordinerede sektorbaserede risikovurderinger af forsyningskæden, som det allerede er sket for 5G-net i henhold til henstilling (EU) 2019/534 om cybersikkerhed i 5G-net[21] med henblik på inden for hver enkelt sektor at identificere de kritiske IKT-tjenester, -systemer eller -produkter, relevante trusler og sårbarheder.

---

[21] Kommissionens henstilling (EU) 2019/534 af 26. marts 2019 Cybersikkerheden i forbindelse med 5G-net (EUT L 88 af 29.3.2019, s. 42).

(47) Ved risikovurderingen af forsyningskæden bør der i lyset af kendetegnene ved den pågældende sektor tages hensyn til både tekniske og, hvor det er relevant, ikketekniske faktorer, herunder dem, der er defineret i henstilling (EU) 2019/534, i den EU-dækkende koordinerede risikovurdering af 5G-netsikkerhed og i EU-værktøjskassen om 5G-cybersikkerhed, som samarbejdsgruppen er nået til enighed om. For at udpege de forsyningskæder, der bør gøres til genstand for en koordineret risikovurdering, bør følgende kriterier tages i betragtning: i) i hvilket omfang væsentlige og vigtige enheder anvender og er afhængige af specifikke kritiske IKT-tjenester, -systemer eller -produkter, ii) relevansen af specifikke kritiske IKT-tjenester, -systemer eller -produkter til udførelse af kritiske eller følsomme funktioner, herunder behandling af personoplysninger, iii) adgangen til alternative IKT-tjenester, -systemer eller -produkter, iv) modstandsdygtigheden i den samlede forsyningskæde for IKT-tjenester, -systemer eller -produkter over for afbrydelser og v) for nye IKT-tjenester, -systemer eller -produkter, deres potentielle fremtidige betydning for enhedernes aktiviteter.

(48) For at strømline de retlige forpligtelser, der pålægges udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester og tillidstjenesteydere i forbindelse med sikkerheden i deres net- og informationssystemer, og for at gøre det muligt for disse enheder og deres respektive kompetente myndigheder at drage fordel af de retlige rammer, der er fastsat i dette direktiv (herunder udpegelse af en CSIRT, der er ansvarlig for risiko- og hændelseshåndtering, kompetente myndigheders og organers deltagelse i samarbejdsgruppens og CSIRT-netværkets arbejde), bør de være omfattet af dette direktivs anvendelsesområde. De tilsvarende bestemmelser i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014[22] og Europa-Parlamentets og Rådets direktiv (EU) 2018/1972[23] vedrørende indførelse af sikkerhedskrav og underretningspligt for disse typer enheder bør derfor ophæves.

---

[22] Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

[23] Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EUT L 321 af 17.12.2018, s. 36).

(48a) **De sikkerhedsforpligtelser, der er fastsat i dette direktiv, bør betragtes som et supplement til de krav, der pålægges tillidstjenesteudbydere i henhold til forordning (EU) nr. 910/2014 (eIDAS-forordningen). Tillidstjenesteudbydere bør anmodes om at træffe alle passende og forholdsmæssige foranstaltninger for at styre de risici, der er forbundet med deres tjenester, herunder i forhold til kunder og modtagertredjeparter, og rapportere sikkerhedshændelser i henhold til dette direktiv. Sådanne sikkerheds- og rapporteringsforpligtelser bør også vedrøre den fysiske beskyttelse af den udbudte tjeneste. Artikel 24 i forordning (EU) nr. 910/2014 finder fortsat anvendelse.**

(48aa) **Medlemsstaterne kan tildele rollen som kompetente myndigheder for tillidstjenester til eIDAS-tilsynsorganerne for at sikre videreførelsen af den nuværende praksis og bygge videre på den viden og erfaring, der er opnået i forbindelse med anvendelsen af eIDAS-forordningen. Hvis denne rolle tildeles et andet organ, bør de nationale kompetente myndigheder i henhold til dette direktiv samarbejde tæt og rettidigt ved at udveksle relevante oplysninger for at sikre effektivt tilsyn med tillidstjenesteudbyderne og sikre deres overholdelse af kravene i dette direktiv og forordning [XXXX/XXXX].**

Hvis det er relevant, bør den nationale kompetente myndighed i henhold til dette direktiv straks underrette eIDAS-tilsynsorganet om enhver underretning om en væsentlig cybertrussel eller -hændelse med indvirkning på tillidstjenester samt om en tillidstjenesteudbyders manglende overholdelse af kravene i henhold til dette direktiv. Med henblik på rapportering kan medlemsstaterne, hvor det er relevant, anvende det fælles kontaktpunkt, der er oprettet for at opnå en fælles og automatisk rapportering om hændelser til både eIDAS-tilsynsorganet og den kompetente myndighed i henhold til dette direktiv. Reglerne om rapporteringsforpligtelser bør ikke berøre forordning (EU) 2016/679 og Europa-Parlamentets og Rådets direktiv 2002/58/EF[24].

---

[24] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

(49) Hvor det er hensigtsmæssigt og for at undgå unødige afbrydelser, bør eksisterende nationale retningslinjer [...], der er vedtaget med henblik på gennemførelse af reglerne vedrørende sikkerhedsforanstaltninger i artikel 40[...] og artikel 41 i direktiv (EU) 2018/1972[...] **tages i betragtning i de ordninger, som medlemsstaterne gennemfører vedrørende dette direktiv, så der bygges på den viden og de færdigheder, der allerede er erhvervet i henhold til direktiv (EU) 2018/1972 vedrørende cybersikkerhedsrisici og hændelsesunderretninger. ENISA kan også udarbejde en vejledning om sikkerheds- og rapporteringskrav for udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester for at fremme harmonisering og overgang og minimere forstyrrelser. Medlemsstaterne kan tildele rollen som kompetente myndigheder for elektronisk kommunikation til de nationale tilsynsmyndigheder for at sikre videreførelsen af den nuværende praksis og bygge videre på den viden og erfaring, der er opnået i direktiv (EU) 2018/1972.**

(50) I betragtning af nummeruafhængige interpersonelle kommunikationstjenesters stigende betydning er det nødvendigt at sikre, at sådanne tjenester også er omfattet af passende sikkerhedskrav i lyset af deres særlige karakter og økonomiske betydning. Leverandører af sådanne tjenester bør således også garantere et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen. Da udbydere af nummeruafhængige interpersonelle kommunikationstjenester normalt ikke udøver egentlig kontrol over transmissionen af signaler via net, kan risikoen i forbindelse med disse tjenester i visse henseender anses for at være lavere end i forbindelse med traditionelle elektroniske kommunikationstjenester. Det samme gælder interpersonelle kommunikationstjenester, der anvender numre, og som ikke udøver faktisk kontrol over signaltransmission.

(51) Det indre marked er mere afhængigt af internettets funktion end nogensinde før. Næsten alle væsentlige og vigtige enheders tjenester er afhængige af tjenester, der leveres over internettet. For at sikre en problemfri levering af tjenester, der udbydes af væsentlige og vigtige enheder, er det vigtigt, at offentlige elektroniske kommunikationsnet, som f.eks. internetbasisnettet eller undersøiske kommunikationskabler, har indført passende cybersikkerhedsforanstaltninger og foretager underretninger om hændelser i forbindelse hermed.

(52) Hvor det er [...] **relevant**, bør enheder underrette deres tjenestemodtagere om de særlige [...] foranstaltninger, de kan træffe for at afbøde den deraf følgende risiko **fra en væsentlig cybertrussel** mod dem selv. **Enhederne bør, hvis det er hensigtsmæssigt, og navnlig i tilfælde, hvor den væsentlige cybertrussel kan blive til virkelighed, også underrette deres tjenestemodtagere parallelt med de kompetente myndigheder eller CSIRT'er om selve truslen.** Kravet om at underrette disse modtagere om sådanne trusler bør ikke fritage enhederne for forpligtelsen til for egen regning at træffe passende og øjeblikkelige foranstaltninger til at forebygge eller afhjælpe eventuelle cybertrusler og genoprette tjenestens normale sikkerhedsniveau. Sådanne oplysninger om **cyber**[...]trusler bør stilles gratis til rådighed for modtagerne.

(53) Det gælder navnlig, at udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester bør informere modtagerne af tjenesten om særlige og væsentlige trusler og om, hvordan de kan sikre deres kommunikation, f.eks. ved at anvende bestemte typer software eller krypteringsteknologier.

(54) For at beskytte sikkerheden i elektroniske kommunikationsnet og -tjenester bør brugen af kryptering, navnlig end-to-end-kryptering, fremmes og om nødvendigt være obligatorisk for udbydere af sådanne tjenester og net i overensstemmelse med principperne om sikkerhed og privatlivsbeskyttelse gennem standardindstillinger og indbygget privatlivsbeskyttelse med henblik på artikel 18. Brugen af end-to-end-kryptering bør forenes med medlemsstaternes beføjelser til at sikre beskyttelsen af deres væsentlige sikkerhedsinteresser og den offentlige sikkerhed og til at muliggøre efterforskning, afsløring og retsforfølgning af strafbare handlinger i overensstemmelse med EU-retten. Løsninger for lovlig adgang til oplysninger i end-to-end-krypteret kommunikation bør opretholde krypteringens effektivitet med hensyn til at beskytte privatlivets fred og kommunikationssikkerheden og samtidig sikre en effektiv bekæmpelse af kriminalitet.

(55) I dette direktiv fastlægges en totrinstilgang for underretning om hændelser med henblik på at finde den rette balance mellem på den ene side hurtig indberetning, der bidrager til at afbøde den potentielle spredning af hændelser og giver enheder mulighed for at søge støtte, og på den anden side grundig indberetning, der udleder værdifulde erfaringer af individuelle hændelser og med tiden forbedrer individuelle virksomheders og hele sektorers modstandsdygtighed over for cybertrusler. Hvis enheder bliver opmærksomme på en hændelse, bør de være forpligtet til at indsende en første underretning inden for 24 timer efterfulgt af en endelig rapport senest en måned efter. Den første underretning bør kun indeholde de oplysninger, der er strengt nødvendige for at gøre de kompetente myndigheder opmærksomme på hændelsen og give enheden mulighed for at søge bistand, hvis det er nødvendigt. En sådan underretning bør, hvor det er relevant, angive, om hændelsen formodes at være forårsaget af ulovlige eller ondsindede handlinger. Medlemsstaterne bør sikre, at kravet om at foretage denne første underretning ikke fjerner den underrettende enheds ressourcer fra aktiviteter vedrørende håndtering af hændelser, der bør prioriteres. For yderligere at forhindre, at forpligtelser til underretning om hændelser enten omdirigerer ressourcer fra håndtering af hændelser eller på anden måde kan bringe enhedernes indsats i den forbindelse i fare, bør medlemsstaterne også fastsætte, at den pågældende enhed i behørigt begrundede tilfælde og efter aftale med de kompetente myndigheder eller CSIRT'en kan afvige fra fristerne på 24 timer for den første underretning og en måned for den endelige rapport.

(55a) En proaktiv tilgang til cybertrusler er et afgørende element i styring af cybersikkerhedsrisici, som bør sætte de kompetente myndigheder i stand til effektivt at forhindre cybertrusler i at blive til faktiske hændelser, der kan forårsage betydelige materielle eller immaterielle tab. Med henblik herpå er underretning om væsentlige cybertrusler af afgørende betydning.

(56) Væsentlige og vigtige enheder befinder sig ofte i en situation, hvor en bestemt hændelse på grund af dens karakteristika skal indberettes til forskellige myndigheder som følge af underretningspligten i forskellige retsakter. Sådanne tilfælde medfører yderligere byrder og kan også føre til usikkerhed med hensyn til formatet af og procedurerne for sådanne meddelelser. Med henblik herpå og med henblik på at forenkle rapportering af sikkerhedshændelser [...] **kan** medlemsstaterne oprette et fælles kontaktpunkt for alle underretninger, der kræves i henhold til dette direktiv og også i henhold til anden EU-lovgivning såsom forordning (EU) 2016/679 og direktiv 2002/58/EF. ENISA bør i samarbejde med samarbejdsgruppen udvikle fælles underretningsmodeller ved hjælp af retningslinjer, der vil forenkle og strømline de underretningsoplysninger, der kræves i henhold til EU-retten, og mindske byrderne for virksomhederne.

(57) Hvis der er mistanke om, at en hændelse har forbindelse til alvorlige kriminelle aktiviteter i henhold til EU-retten eller national ret, bør medlemsstaterne opfordre væsentlige og vigtige enheder til på grundlag af gældende strafferetsplejeregler i overensstemmelse med EU-retten at indberette hændelser af formodet alvorlig kriminel karakter til de relevante retshåndhævende myndigheder. Hvor det er relevant, og uden at det berører de regler om beskyttelse af personoplysninger, der gælder for Europol, er det ønskeligt, at EC3 og ENISA letter koordineringen mellem de kompetente myndigheder og de retshåndhævende myndigheder i forskellige medlemsstater.

(58) Personoplysninger bliver i mange tilfælde kompromitteret som følge af hændelser. I denne forbindelse bør de kompetente myndigheder samarbejde og udveksle oplysninger om alle relevante spørgsmål med databeskyttelsesmyndighederne og tilsynsmyndighederne i henhold til direktiv 2002/58/EF.

(59) Det er afgørende at vedligeholde nøjagtige og fuldstændige databaser over domænenavne og registreringsdata (såkaldte "WHOIS-data") og give lovlig adgang til sådanne data for at sikre DNS'ens sikkerhed, stabilitet og modstandsdygtighed, hvilket igen bidrager til et højt fælles cybersikkerhedsniveau i Unionen. Hvis behandlingen omfatter personoplysninger, skal denne behandling være i overensstemmelse med EU's databeskyttelseslovgivning.

(60) Offentlige myndigheders, herunder kompetente myndigheder i henhold til EU-retten eller national ret med henblik på forebyggelse, efterforskning eller retsforfølgning af strafbare handlinger, CERT'er, [...]CSIRT'er og for så vidt angår deres kunders data til udbydere af elektroniske kommunikationsnet og -tjenester og udbydere af cybersikkerhedsteknologier og -tjenester, der handler på vegne af disse kunder, mulighed for at tilgå og få rettidig adgang til disse data er afgørende for at forebygge og bekæmpe misbrug af domænenavnesystemet, navnlig for at forebygge, opdage og reagere på cybersikkerhedshændelser. En sådan adgang bør ske i overensstemmelse med EU's databeskyttelseslovgivning, for så vidt som den vedrører personoplysninger.

(61) For at sikre, at der er adgang til nøjagtige og fuldstændige data til registrering af domænenavne, bør topdomæneadministratorer og enheder, der udbyder domænenavnsregistreringstjenester til topdomæner (såkaldte registratorer), indsamle og garantere integriteten og tilgængeligheden af registreringsdata for domænenavne. **For så vidt angår registreringsdata bør enhederne navnlig kontrollere registrantens navn og e-mailadresse.** Topdomæneadministratorer og enheder, der udbyder domænenavneregistreringstjenester til topdomæner, bør [...] fastlægge politikker og procedurer for indsamling og vedligeholdelse af nøjagtige og fuldstændige registreringsdata samt for at forhindre og korrigere unøjagtige registreringsdata i overensstemmelse med EU's databeskyttelsesregler.

(62) Topdomæneadministratorer og enheder, der udbyder domænenavnsregistreringstjenester til dem, bør offentliggøre domænenavnsregistreringsdata, der falder uden for anvendelsesområdet for EU's databeskyttelsesregler, såsom data, der vedrører juridiske personer[25]. Topdomæneadministratorer og enheder, der udbyder domænenavneregistreringstjenester til topdomæner, bør også give legitime adgangssøgende lovlig adgang til specifikke domænenavnsregistreringsdata om fysiske personer i overensstemmelse med EU's databeskyttelseslovgivning. Medlemsstaterne bør sikre, at topdomæneadministratorer og enheder, der udbyder domænenavnsregistreringstjenester til dem, uden unødig forsinkelse besvarer anmodninger [...] om videregivelse af domænenavnsregistreringsdata **fra legitime adgangssøgende, som f.eks. kompetente myndigheder i henhold til EU-retten eller national ret på området national sikkerhed og strafferet eller CSIRT'er**. Topdomæneadministratorer og de enheder, der udbyder domænenavnsregistreringstjenester til dem, bør fastlægge politikker og procedurer for offentliggørelse og fremlæggelse af registreringsdata, herunder serviceleveranceaftaler til behandling af anmodninger om adgang fra legitime adgangssøgende. Adgangsproceduren kan også omfatte brug af en grænseflade, en portal eller et andet teknisk værktøj til at tilvejebringe et effektivt system til anmodning om og adgang til registreringsdata. **Medlemsstaterne bør sikre, at alle former for adgang til domæneregistreringsdata (både personoplysninger og andre oplysninger end personoplysninger) er gratis.** Med henblik på at fremme en harmoniseret praksis i hele det indre marked kan Kommissionen vedtage retningslinjer for sådanne procedurer, uden at dette berører Det Europæiske Databeskyttelsesråds beføjelser, **i overensstemmelse med og som supplement til internationale standarder, der er udviklet af multiinteressentsamfundet**.

---

[25] Europa-Parlamentets og Rådets forordning (EU) 2016/679**,** betragtning 14: "Denne forordning finder ikke anvendelse på behandling af personoplysninger, der vedrører juridiske personer, navnlig virksomheder, der er etableret som juridiske personer, herunder den juridiske persons navn, form og kontaktoplysninger".

(63) [...]**V**æsentlige og vigtige enheder i henhold til dette direktiv bør henhøre under jurisdiktionen i den medlemsstat, hvor de leverer deres tjenester. **De enheder, der er omhandlet i punkt 1-7 og punkt 10 i bilag I, tillidstjenesteudbydere og udbydere af internetudvekslingspunkter, der er omhandlet i punkt 8 i bilag I, og punkt 1-5 i bilag II til dette direktiv, bør henhøre under jurisdiktionen i den medlemsstat, hvor de er etableret.** Hvis enheden leverer tjenester **eller har en virksomhed** i mere end én medlemsstat, bør den henhøre under hver af disse medlemsstaters særskilte og parallelle jurisdiktion. De kompetente myndigheder i disse medlemsstater bør samarbejde, yde gensidig bistand til hinanden og, hvor det er relevant, gennemføre fælles tilsynsforanstaltninger. **Hvis medlemsstaterne beslutter at udøve kompetencen, bør de undgå, at den samme adfærd straffes mere end én gang for overtrædelse af de forpligtelser, der er fastsat i dette direktiv.**

(64) For at tage hensyn til den grænseoverskridende karakter af DNS-tjenesteudbyderes tjenester og operationer, topdomænenavneadministratorer, **enheder, der udbyder domænenavnsregistreringstjenester til topdomæner,** udbydere af indholdsleveringsnetværk, udbydere af cloudcomputingtjenester, datacentertjenesteudbydere og digitale udbydere bør kun én medlemsstat have jurisdiktion over disse enheder. Jurisdiktionen bør tillægges den medlemsstat, hvor den pågældende enhed har sit hovedsæde i Unionen. Etableringskriteriet i dette direktiv indebærer faktisk udøvelse af virksomhed gennem faste ordninger. De pågældende ordningers juridiske form, hvad enten der er tale om en filial eller et datterselskab med status som juridisk person, har ikke afgørende betydning i denne forbindelse.

Dette kriterium bør ikke afhænge af, hvorvidt net- og informationssystemerne fysisk befinder sig på et givent sted. Tilstedeværelsen og anvendelsen af sådanne systemer udgør ikke i sig selv et sådant hjemsted og er derfor ikke et kriterium for fastlæggelse af hjemstedet. Hovedvirksomheden bør være det sted, hvor beslutningerne vedrørende foranstaltninger til styring af cybersikkerhedsrisici **overvejende** træffes i Unionen. Dette vil typisk svare til placeringen af selskabernes centrale administration i Unionen. Hvis **det sted, hvor sådanne beslutninger overvejende træffes, ikke kan fastslås, eller** sådanne beslutninger ikke træffes i Unionen, bør hovedvirksomheden anses for at befinde sig i de medlemsstater, hvor enheden har en virksomhed med det største antal ansatte i Unionen. Når tjenesterne udføres af en gruppe af virksomheder, bør den kontrollerende virksomheds hovedvirksomhed anses for at være gruppen af virksomheders hovedvirksomhed.

(64a) Når en rekursiv DNS-tjeneste kun udbydes af en udbyder af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som en del af internetadgangstjenesten, bør enheden anses for at være underlagt jurisdiktionen i alle de medlemsstater, hvor dens tjenester udbydes.

(64aa) For at sikre et klart overblik over DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der udbyder domænenavnsregistreringstjenester til topdomæner, udbydere af indholdsleveringsnetværk, udbydere af cloudcomputingtjenester, datacentertjenesteudbydere og digitale udbydere, der udbyder tjenester i hele Unionen inden for rammerne af dette direktiv, bør ENISA oprette og føre et register over disse enheder på grundlag af underretninger, som medlemsstaterne modtager, alt efter omstændighederne via deres nationale mekanismer for selvunderretning. Med henblik på at sikre, at de oplysninger, der bør medtages i dette register, er nøjagtige og fuldstændige, bør medlemsstaterne forelægge ENISA de oplysninger, der findes i deres nationale registre om disse enheder. ENISA og medlemsstaterne bør træffe foranstaltninger til at fremme interoperabiliteten mellem sådanne registre og samtidig sikre beskyttelse af fortrolige eller klassificerede informationer.

(65) I tilfælde, hvor en DNS-tjenesteudbyder, et topdomænenavneadministrator, en udbyder af indholdsudsendelsesnetværk, en udbyder af cloudcomputingtjenester, en datacentertjenesteudbyder og en digital udbyder, der ikke er etableret i Unionen, udbyder tjenester i Unionen, bør denne udpege en repræsentant. Med henblik på at afgøre, om en sådan udbyder af digitale tjenester tilbyder tjenester i Unionen, bør det fastslås, om det er åbenbart, at udbyderen af digitale tjenester påtænker at tilbyde tjenester til personer i en eller flere medlemsstater. Alene det forhold, at der i Unionen er adgang til udbyderen af digitale tjenesters eller en mellemmands websted eller til en e-mailadresse og andre kontaktoplysninger, eller at der benyttes et sprog, som almindeligvis benyttes i det tredjeland, hvor enheden er etableret, er ikke tilstrækkeligt til at fastslå en sådan hensigt. Imidlertid kan faktorer såsom anvendelse af et sprog eller en valuta, der almindeligvis anvendes i en eller flere medlemsstater med mulighed for at bestille tjenester på det pågældende sprog, eller omtale af kunder eller brugere, der befinder sig i Unionen, gøre det åbenbart, at udbyderen af enhed påtænker at tilbyde tjenester i Unionen. Repræsentanten bør handle på vegne af enheden, og kompetente myndigheder eller CSIRT'er bør kunne kontakte repræsentanten. Repræsentanten bør udtrykkeligt udpeges ved et skriftligt mandat fra udbyderen af digitale tjenester til at handle på sidstnævntes vegne for så vidt angår sidstnævntes forpligtelser i medfør af dette direktiv, herunder underretning om hændelser.

(66) Hvis oplysninger, der betragtes som klassificerede i henhold til national ret eller EU-retten, udveksles, indberettes eller på anden måde deles i henhold til bestemmelserne i dette direktiv, bør de tilsvarende specifikke regler for håndtering af klassificerede oplysninger finde anvendelse.

(67) I takt med at cybertruslerne bliver mere komplekse og sofistikerede, er gode detektions- og forebyggelsesforanstaltninger i høj grad afhængige af regelmæssig udveksling af trussels- og sårbarhedsefterretninger mellem enheder. Informationsudveksling bidrager til øget bevidsthed om cybertrusler, hvilket igen styrker finansielle enheders evne til at forhindre trusler i at blive til faktiske hændelser og sætter enhederne i stand til bedre at inddæmme virkningerne af hændelser og foretage en mere effektiv genopretning. Da der ikke findes nogen retningslinjer på EU-plan, synes flere faktorer at have hæmmet en sådan udveksling af efterretninger, navnlig usikkerhed om foreneligheden med databeskyttelsesregler, antitrustregler og regler om ansvar.

(68) Enheder bør tilskyndes til i fællesskab at øge deres individuelle viden og praktiske erfaring på strategisk, taktisk og operationelt plan med henblik på at styrke deres kapacitet til i tilstrækkeligt omfang at vurdere, overvåge, forsvare sig mod og reagere på cybertrusler. Det er derfor nødvendigt at gøre det muligt at etablere mekanismer på EU-plan for frivillige ordninger for udveksling af oplysninger. Med henblik herpå bør medlemsstaterne aktivt støtte og tilskynde også relevante enheder, der ikke er omfattet af dette direktivs anvendelsesområde, til at deltage i sådanne informationsudvekslingsmekanismer. Disse mekanismer bør gennemføres i fuld overensstemmelse med Unionens konkurrenceregler og EU-rettens regler om databeskyttelse.

(69) [...] **I** det omfang det er strengt nødvendigt og står i et rimeligt forhold til målet om at sikre net- og informationssikkerhed **kan behandling af personoplysninger** hos **væsentlige og vigtige** enheder [...] og udbydere af sikkerhedsteknologier og -tjenester **blive anset for nødvendig for at overholde en retlig forpligtelse eller** [...] udgøre en legitim interesse for den pågældende dataansvarlige**[...]**, jf. forordning (EU) 2016/679. Dette **kan** [...] omfatte foranstaltninger vedrørende forebyggelse, opdagelse, analyse og reaktion på hændelser, foranstaltninger til at øge bevidstheden i forbindelse med specifikke cybertrusler, udveksling af oplysninger i forbindelse med afhjælpning af sårbarheder og koordineret videregivelse samt frivillig udveksling af oplysninger om disse hændelser, [...] cybertrusler og sårbarheder, kompromitteringsindikatorer, taktikker, teknikker og procedurer, cybersikkerhedsadvarsler og konfigurationsværktøjer. Sådanne foranstaltninger kan kræve behandling af [...] **forskellige** typer personoplysninger **såsom**: IP-adresser, uniform resources locators (URL'er), domænenavne og e-mailadresser. **Kompetente myndigheders, SPOC'ers og CSIRT'ers behandling af personoplysninger bør fastsættes i national ret og anses for nødvendig for at overholde en retlig forpligtelse eller for at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, jf. artikel 6, stk. 1, litra c) eller e), i forordning (EU) 2016/679**.

(69a) Medlemsstaternes lovgivning kan fastsætte regler, der gør det muligt for de kompetente myndigheder, SPOC'er og CSIRT'er, i det omfang det er strengt nødvendigt og rimeligt for at garantere sikkerheden i væsentlige og vigtige enheders net- og informationssystemer, at behandle særlige kategorier af personoplysninger i overensstemmelse med artikel 9[...] i forordning (EU) 2016/679, navnlig ved at fastsætte passende og specifikke foranstaltninger til beskyttelse af fysiske personers grundlæggende rettigheder og interesser, herunder tekniske begrænsninger for videreanvendelse af sådanne data og anvendelsen af de mest avancerede sikkerhedsforanstaltninger og foranstaltninger til beskyttelse af privatlivets fred, f.eks. pseudonymisering, eller kryptering, hvis anonymisering i væsentlig grad kan påvirke det tilstræbte formål.

(70) For at styrke de tilsynsbeføjelser og -foranstaltninger, der bidrager til at sikre effektiv overholdelse, bør dette direktiv indeholde en minimumsliste over tilsynsforanstaltninger og -midler, hvorigennem de kompetente myndigheder **kan** [...] føre tilsyn med væsentlige og vigtige enheder. Desuden bør der ved dette direktiv indføres en differentiering af tilsynsordningen mellem væsentlige og vigtige enheder med henblik på at sikre en rimelig balance mellem forpligtelser for både enheder og kompetente myndigheder. Væsentlige enheder bør derfor være underlagt en fuldt udbygget tilsynsordning (forudgående og efterfølgende), mens vigtige enheder bør være underlagt en lempelig tilsynsordning, som kun gælder efterfølgende. For sidstnævnte betyder dette, at vigtige enheder ikke systematisk bør **være forpligtet til**[...] at **dokumentere** overholdelsen af kravene for styring af cybersikkerhedsrisici, mens de kompetente myndigheder bør anvende en reaktiv efterfølgende tilgang til tilsyn og dermed ikke have en generel forpligtelse til at føre tilsyn med disse enheder. **For vigtige enheder kan efterfølgende tilsyn udløses af dokumentation eller enhver indikation eller oplysning, som de kompetente myndigheder gøres opmærksom på, og som de anser for at indikere en potentiel manglende overholdelse af de forpligtelser, der er fastsat i dette direktiv. En sådan dokumentation eller sådanne indikationer eller oplysninger kan f.eks. være af den type, som de kompetente myndigheder modtager fra andre myndigheder, enheder, borgere, medier eller andre kilder, offentligt tilgængelige oplysninger, eller de kan hidrøre fra andre aktiviteter, der udføres af de kompetente myndigheder som led i udførelsen af deres opgaver.**

(70a) I forbindelse med udøvelsen af forudgående tilsyn bør de kompetente myndigheder kunne træffe afgørelse om prioriteringen af anvendelsen af tilsynsforanstaltninger og -midler, som de har til rådighed, på en forholdsmæssig måde. Dette indebærer, at de kompetente myndigheder kan træffe afgørelse om en sådan prioritering på grundlag af tilsynsmetoder, som bør følge en risikobaseret tilgang. Mere specifikt kan disse metoder omfatte kriterier eller benchmarks for klassificering af væsentlige enheder i risikokategorier og tilsvarende tilsynsforanstaltninger og anbefalede midler pr. risikokategori, som f.eks. anvendelse, hyppighed eller type af kontrol på stedet eller målrettede sikkerhedsrevisioner eller sikkerhedsscanninger, typer af oplysninger, der skal anmodes om, og detaljeringsgraden af disse oplysninger. Disse tilsynsmetoder kan også ledsages af arbejdsprogrammer og vurderes og revideres regelmæssigt, herunder aspekter som ressourceallokering og -behov.

(70aa) For så vidt angår offentlige forvaltningsorganer bør tilsynsbeføjelserne udøves i overensstemmelse med de nationale rammer og det nationale retssystem. Medlemsstaterne bør kunne beslutte at indføre passende, forholdsmæssige og effektive tilsyns- og håndhævelsesforanstaltninger vedrørende disse enheder.

(70aaa) For at påvise overensstemmelse med visse foranstaltninger til styring af cybersikkerhedsrisici kan medlemsstaterne kræve, at væsentlige og vigtige enheder anvender kvalificerede tillidstjenester eller anmeldte elektroniske identifikationsordninger i henhold til forordning (EU) nr. 910/2014.

(71) For at gøre håndhævelsen effektiv bør der fastlægges en minimumsliste over administrative sanktioner for brud på forpligtelserne vedrørende styring af cybersikkerhedsrisici og rapportering i dette direktiv, som opstiller en klar og konsekvent ramme for sådanne sanktioner i hele Unionen. Der bør tages behørigt hensyn til overtrædelsens art, grovhed og varighed, den faktiske skade eller de lidte tab eller potentielle skader eller tab, der kunne være blevet udløst, overtrædelsens forsætlige eller uagtsomme karakter, de foranstaltninger, der er truffet for at forebygge eller begrænse den lidte skade og/eller de lidte tab, graden af ansvar eller eventuelle relevante tidligere overtrædelser, graden af samarbejde med den kompetente myndighed og enhver anden skærpende eller formildende omstændighed. Pålæggelse af sanktioner, herunder administrative bøder, bør være omfattet af fornødne proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og Den Europæiske Unions charter om grundlæggende rettigheder, herunder effektiv retsbeskyttelse og en retfærdig rettergang.

(71a) Bestemmelserne om ansvar for fysiske personer, der har visse ansvarsområder inden for en enhed, i forbindelse med tilsidesættelse af deres forpligtelse til at sikre overholdelse af forpligtelserne i dette direktiv, kræver ikke, at medlemsstaterne sørger for strafferetlig forfølgning eller civilretligt ansvar for skader forårsaget af en sådan tilsidesættelse over for tredjemand.

(72) For at sikre en effektiv håndhævelse af de forpligtelser, der er fastsat i dette direktiv, bør hver kompetent myndighed have beføjelse til at pålægge eller anmode om pålæggelse af administrative bøder.

(73) Når en virksomhed pålægges administrative bøder, forstås en virksomhed i denne forbindelse som en virksomhed som omhandlet i artikel 101 og 102 i TEUF. Når personer, der ikke er en virksomhed, pålægges administrative bøder, bør tilsynsmyndigheden i forbindelse med fastsættelsen af bødestørrelsen tage hensyn til det generelle indkomstniveau i den pågældende medlemsstat og personens økonomiske situation. Det bør være op til medlemsstaterne at bestemme, om og i hvilket omfang de offentlige myndigheder bør kunne pålægges administrative bøder. Pålæggelse af en administrativ bøde berører ikke de kompetente myndigheders anvendelse af andre beføjelser eller andre sanktioner, der er fastsat i de nationale regler til gennemførelse af dette direktiv.

(74) Medlemsstaterne [...] **kan** fastsætte regler om strafferetlige sanktioner for overtrædelse af de nationale regler til gennemførelse af dette direktiv. Pålæggelse af strafferetlige sanktioner for overtrædelse af sådanne nationale regler og tilknyttede administrative sanktioner bør dog ikke føre til et brud på ne bis in idem-princippet som fortolket af EU-Domstolen.

(75) Når dette direktiv ikke harmoniserer administrative sanktioner eller om nødvendigt i andre tilfælde, f.eks. i tilfælde af alvorlige overtrædelser af forpligtelser, der er fastsat i dette direktiv, bør medlemsstaterne indføre en ordning, der giver mulighed for at pålægge sanktioner, som er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning. Sanktionernes art, strafferetlige eller administrative, bør fastsættes i medlemsstaternes nationale ret.

(76) For yderligere at styrke effektiviteten og den afskrækkende virkning af de sanktioner, der finder anvendelse på overtrædelser af forpligtelser, der er fastsat i henhold til dette direktiv, bør de kompetente myndigheder have beføjelse til at anvende sanktioner, der består i at suspendere en certificering eller tilladelse vedrørende en væsentlig enheds tjenester eller dele heraf og indføre et midlertidigt forbud mod en fysisk persons udøvelse af ledelsesfunktioner. I betragtning af deres alvor og indvirkning på enhedernes aktiviteter og i sidste ende på deres forbrugere bør sådanne sanktioner kun anvendes proportionalt med overtrædelsens alvor og under hensyntagen til de særlige omstændigheder i den enkelte sag, herunder overtrædelsens forsætlige eller uagtsomme karakter, foranstaltninger, der træffes for at forebygge eller begrænse den lidte skade og/eller de lidte tab. Sådanne sanktioner bør kun anvendes som ultima ratio, dvs. kun efter at de øvrige relevante håndhævelsesforanstaltninger, der er fastsat i dette direktiv, er udtømt, og kun indtil de enheder, de pålægges, træffer de nødvendige foranstaltninger for at afhjælpe manglerne eller opfylde kravene fra den kompetente myndighed, for hvilken sådanne sanktioner er blevet anvendt. Pålæggelse af sådanne sanktioner skal være underlagt fornødne proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og Den Europæiske Unions charter om grundlæggende rettigheder, herunder effektiv retsbeskyttelse, retfærdig rettergang, uskyldsformodning og retten til et forsvar.

(76a) For at sikre et effektivt tilsyn og en effektiv håndhævelse, særligt i sager med en grænseoverskridende dimension, bør medlemsstater, der har modtaget en anmodning om gensidig bistand, i anmodningens omfang træffe passende tilsyns- og håndhævelsesforanstaltninger over for den pågældende enhed, der udbyder tjenester, eller som har net- og informationssystemet på deres område.

(77) Dette direktiv bør fastlægge samarbejdsregler mellem de kompetente myndigheder og tilsynsmyndighederne i overensstemmelse med forordning (EU) 2016/679 om behandling af overtrædelser vedrørende personoplysninger.

(78) Dette direktiv bør sigte mod at sikre et højt ansvarsniveau for risikohåndteringsforanstaltninger og rapporteringsforpligtelser i forbindelse med cybersikkerhed på organisationsniveau. Derfor bør ledelsesorganerne for de enheder, der er omfattet af dette direktiv, godkende foranstaltningerne vedrørende cybersikkerhedsrisici og føre tilsyn med deres gennemførelse.

(79) Der bør indføres et peer[...] **lærings**[...]**system for at bidrage til at styrke den gensidige** tillid **og tage ved lære af god praksis og erfaringer**, som muliggør [...] **peerudvekslinger** mellem eksperter udpeget af medlemsstaterne o**m**[...] gennemførelsen af cybersikkerhedspolitikker[...]. **Ved gennemførelsen af peerlæringssystemet bør der lægges særlig vægt på at sikre, at det ikke pålægger de relevante medlemsstaters myndigheder en unødvendig eller uforholdsmæssigt stor byrde. Kommissionen bør undersøge alle muligheder for potentielt at garantere, at der er finansiel dækning for de omkostninger, der kan være forbundet med tilrettelæggelsen af peerlæringsmissioner. Desuden bør peerlæringssystemet tage hensyn til resultaterne af lignende mekanismer, såsom CSIRT-netværkets peerevalueringssystem, tilføre merværdi og undgå overlapning. Gennemførelsen af peerlæringssystemet bør ikke berøre national ret eller EU-retten om beskyttelse af fortrolige og klassificerede informationer. Inden peerlæringsrunderne påbegyndes, kan medlemsstaterne foretage en selvevaluering af de relevante aspekter. Efter anmodning fra samarbejdsgruppen kan ENISA om nødvendigt give vejledning om selvevaluering og relevante skabeloner. Medlemsstaterne kan beslutte at gøre deres respektive rapporter offentligt tilgængelige.**

(80) [...]

(81) For at sikre ensartede betingelser for gennemførelsen af de relevante bestemmelser i dette direktiv vedrørende de proceduremæssige ordninger, der er nødvendige for samarbejdsgruppens funktion, de tekniske elementer vedrørende risikostyringsforanstaltninger eller typen af oplysninger, formatet og proceduren for underretning af hændelser, **de kategorier af enheder, der skal anvende visse certificerede IKT-produkter, -tjenester og -processer** bør Kommissionen tillægges gennemførelsesbeføjelser. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011[26].

(82) Kommissionen bør regelmæssigt tage dette direktivs bestemmelser op til fornyet overvejelse efter høring af interesserede parter, navnlig med henblik på at afgøre, om der er behov for ændringer i lyset af skiftende samfundsmæssige, politiske eller teknologiske vilkår eller markedsvilkår.

---

[26] Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).

(83) Eftersom målene for dette direktiv, nemlig at opnå et højt, fælles sikkerhedsniveau i net- og informationssystemer i Unionen, ikke i tilstrækkelig grad kan opfyldes af medlemsstaterne, men på grund af handlingens virkninger bedre kan nås på EU-plan, kan Unionen derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går dette direktiv ikke videre, end hvad der er nødvendigt for at nå disse mål.

(84) Dette direktiv overholder de grundlæggende rettigheder og de principper, der anerkendes i Den Europæiske Unions charter om grundlæggende rettigheder, navnlig retten til respekt for privatlivet og kommunikation, beskyttelsen af personoplysninger, frihed til at oprette og drive egen virksomhed, ejendomsretten og retten til effektive retsmidler for en domstol og retten til at blive hørt. Direktivet bør gennemføres i overensstemmelse med disse rettigheder og principper —

VEDTAGET DETTE DIREKTIV:

KAPITEL I

Generelle bestemmelser

Artikel 1

Genstand

1. Dette direktiv fastsætter foranstaltninger med henblik på at sikre et højt fælles cybersikkerhedsniveau i Unionen **for at forbedre det indre markeds funktion**.

2. Med henblik herpå gælder det for dette direktiv, at:

   a) det fastsætter forpligtelser for medlemsstaterne til at vedtage nationale cybersikkerhedsstrategier, udpege kompetente nationale myndigheder, centrale kontaktpunkter og enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)

   b) det fastsætter forpligtelser vedrørende risikostyring og rapportering om cybersikkerhedsrisici for enheder af en type, der er omhandlet [...] i bilag **I og II** [...]

   c) det fastsætter **regler og** forpligtelser vedrørende udveksling af cybersikkerhedsoplysninger.

Artikel 2

Anvendelsesområde

1. Dette direktiv finder anvendelse på offentlige og private enheder af de type**r**, **der fremgår**[...] af [...] bilag **I og II** [...]**, som når eller overstiger lofterne for mellemstore virksomheder** [...], jf. Kommissionens henstilling 2003/361/EF[27]. **Artikel 3, stk. 4, og artikel 6, stk. 2, andet og tredje afsnit, i bilaget til nævnte henstilling finder ikke anvendelse inden for rammerne af dette direktiv.**

2. [...]**U**anset [...] størrelsen **på de enheder, der er omhandlet i stk. 11**, finder dette direktiv også anvendelse**, hvis**: [...]

   a) tjenesterne leveres af en af følgende enheder:

      (i) **udbydere af** offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som omhandlet i bilag I, punkt 8

      (ii) **kvalificerede tillidstjenesteudbydere som omhandlet i bilag I, punkt XX**

      iii) **ikkekvalificerede tillidstjenesteudbydere som omhandlet i bilag I, punkt XX**

      iv) topdomænenavneadministratorer [...], jf. bilag I, punkt 8

   b) [...]

---

[27] Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

c) enheden er den eneste udbyder **i en medlemsstat** af en tjeneste [...]**, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter**

d) en potentiel forstyrrelse af den tjeneste, enheden leverer, kan have [...] **væsentlig** indvirkning på den offentlige sikkerhed eller folkesundheden

e) en potentiel forstyrrelse af den tjeneste, der leveres af enheden, kan medføre [...] **væsentlige** systemiske risici, navnlig for de sektorer, hvor en sådan forstyrrelse kan have en grænseoverskridende virkning

f) [...]

g) enheden identificeres som en kritisk enhed i henhold til Europa-Parlamentets og Rådets direktiv (EU) XXXX/XXXX[28] [direktivet om kritiske enheders modstandsdygtighed] **[**eller som en enhed svarende til en kritisk enhed i henhold til nævnte direktivs artikel 7**]**.

2a. **Uanset deres størrelse finder dette direktiv også anvendelse på centralregeringers offentlige forvaltningsenheder, der er anerkendt som sådanne i en medlemsstat i overensstemmelse med national ret, og som er omhandlet i bilag I, punkt 9. Medlemsstaterne kan fastsætte, at dette direktiv ligeledes finder anvendelse på offentlige forvaltningsenheder på regionalt og lokalt niveau.**

---

[28] [Indsæt den fulde titel og EUT-offentliggørelseshenvisning, når den kendes].

3. [...]

Dette direktiv berører ikke medlemsstaternes ansvar for at beskytte den nationale sikkerhed eller deres beføjelse til at beskytte andre væsentlige statslige funktioner, herunder sikring af statens territoriale integritet og opretholdelse af lov og orden.

3a. 1) Dette direktiv finder ikke anvendelse på:

a) enheder, der falder uden for EU-rettens anvendelsesområde, og under alle omstændigheder alle enheder, som hovedsagelig udfører aktiviteter på områderne forsvar, national sikkerhed eller retshåndhævelse, uanset hvilken enhed der udfører disse aktiviteter, og om den er en offentlig eller en privat enhed, jf. dog stk. 2

b) enheder, der udfører aktiviteter på områderne retsvæsen, parlamenter eller centralbanker. [...]

2) Når offentlige forvaltningsenheder kun udøver aktiviteter på disse områder som led i deres almindelige aktiviteter, er de i deres helhed udelukket fra dette direktivs anvendelsesområde.

3aa. Dette direktiv finder ikke anvendelse på:

i) aktiviteter udført af enheder, der falder uden for EU-rettens anvendelsesområde, og under alle omstændigheder alle aktiviteter, som vedrører national sikkerhed eller forsvar, uanset hvilken enhed der udfører disse aktiviteter, og om den er en offentlig eller en privat enhed

ii) aktiviteter udført af enheder inden for retsvæsenet, parlamenterne, centralbanker og på området offentlig sikkerhed, herunder offentlige forvaltningsenheder, der udfører retshåndhævelsesaktiviteter med henblik på forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner.

3aaa. De forpligtelser, der er fastsat i dette direktiv, indebærer ikke meddelelse af oplysninger, hvis videregivelse strider mod medlemsstaternes væsentlige interesser med hensyn til national sikkerhed, offentlig sikkerhed eller forsvar.

3aaaa. Dette direktiv berører ikke EU-retten om beskyttelse af personoplysninger, særlig forordning (EU) 2016/679 og direktiv 2002/58/EF.

3b. Dette direktiv finder ikke anvendelse på enheder, der er undtaget fra Europa-Parlamentets og Rådets forordning (EU) XXXX/XXXX [DORA-forordningen] i overensstemmelse med artikel 2, stk. 4, i DORA-forordningen.

4. Dette direktiv berører ikke [...][29] [...] Europa-Parlamentets og Rådets direktiv 2011/93/EU[30] og 2013/40/EU[31].

5. Oplysninger, der er fortrolige i henhold til EU-regler og nationale regler, som f.eks. regler om forretningshemmeligheder, udveksles med forbehold af artikel 346 i TEUF kun med Kommissionen og andre relevante myndigheder**, jf. dette direktiv**, hvis en sådan udveksling er nødvendig for anvendelsen af dette direktiv. De udvekslede oplysninger begrænses til, hvad der er relevant og forholdsmæssigt under hensyn til formålet med udvekslingen. Udvekslingen af oplysninger skal sikre de nævnte oplysningers fortrolighed og beskytte sikkerheden og de kommercielle interesser hos væsentlige eller vigtige enheder.

---

[29] [...].

[30] Europa-Parlamentets og Rådets direktiv 2011/93/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi og om erstatning af Rådets rammeafgørelse 2004/68/RIA (EUT L 335 af 17.12.2011, s. 1).

[31] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

Artikel 2a

Væsentlige og vigtige enheder

1. **Af de enheder, som dette direktiv finder anvendelse på, betragtes følgende som væsentlige:**

   i) **enheder af den type, der er omhandlet i bilag I, punkt 1-8a og 10, til dette direktiv, og som overstiger lofterne for mellemstore virksomheder som defineret i Kommissionens henstilling 2003/361/EF**

   ii) **mellemstore enheder omhandlet i artikel 2, stk. 2, litra a), nr. i)**

   iii) **enheder omhandlet i dette direktivs artikel 2, stk. 2, litra a), nr. ii) og iv), uanset størrelse**

   iv) **enheder omhandlet i dette direktivs artikel 2, stk. 2, litra g), og stk. 2a, uanset størrelse**

   v) **enheder, som medlemsstaterne inden dette direktivs ikrafttræden har identificeret som operatører af væsentlige tjenester i overensstemmelse med direktiv (EU) 2016/1148 eller national ret, hvis de er oprettet af medlemsstaterne**

   vi) **enheder, der overskrider lofterne for mellemstore virksomheder som defineret i Kommissionens henstilling 2003/361/EF af den type, der er omhandlet i bilag II, og som medlemsstaterne fastslår er væsentlige ud fra kriterierne i artikel 2, stk. 2, litra c)-e)**

vii) mellemstore enheder som omhandlet i Kommissionens henstilling 2003/361/EF, som medlemsstaterne fastslår er væsentlige ud fra kriterierne i artikel 2, stk. 2, litra c)-e)

viii) mikroenheder eller små enheder som omhandlet i Kommissionens henstilling 2003/361/EF og anført i stk. 2, litra a), nr. i), eller identificeret i medfør af stk. 2, litra c)-e), i denne artikel, og som medlemsstaterne fastslår er væsentlige på grundlag af nationale risikovurderinger.

2. Af de enheder, som dette direktiv finder anvendelse på, betragtes følgende som vigtige:

i) enheder af den type, der er omhandlet i bilag I til dette direktiv, og som kan betegnes som mellemstore virksomheder, jf. Kommissionens henstilling 2003/361/EF[32]**, og enheder af den type, der er omhandlet i bilag II, og som når eller overstiger lofterne for mellemstore virksomheder, jf. henstilling 2003/361/EF**

ii) enheder omhandlet i dette direktivs artikel 2, stk. 2, nr. iii), uanset størrelse

iii) mikroenheder og små enheder omhandlet i artikel 2, stk. 2, litra a), nr. i)

iv) mikroenheder og små enheder, som medlemsstaterne fastslår er vigtige enheder på grundlag af artikel 2, stk. 2, litra c)-e).

---

[32] **Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).**

Artikel 2a

Underretningsordninger

1. **Medlemsstaterne kan indføre en national mekanisme for selvunderretning, som kræver, at alle enheder, der er omfattet af dette direktiv, mindst indgiver deres navn, adresse, kontaktoplysninger, den sektor, de opererer i, eller den type tjeneste, som de udbyder, og, hvor det er relevant, en liste over medlemsstater, hvor de udbyder tjenester, der er omfattet af dette direktiv, til de kompetente myndigheder i henhold til dette direktiv eller til organer, som er udpeget til dette formål af medlemsstaterne.**

2. Medlemsstaterne [...] indgiver **senest [12 måneder efter gennemførelsesfristen for dette direktiv] for så vidt angår de enheder, som de har identificeret i medfør af artikel 2, stk. 2, litra b), litra b)-e), mindst relevante oplysninger om antallet af identificerede enheder, den sektor, som de tilhører, eller den type tjeneste, som de udbyder, jf. bilagene, og den eller de specifikke bestemmelser i artikel 2, stk. 2, på grundlag af hvilke de er identificeret,** til Kommissionen. Medlemsstaterne gennemgår [...] **disse oplysninger** [...] regelmæssigt og derefter mindst hvert andet år og ajourfører dem, hvis det er relevant.

Artikel 2b

Sektorspecifikke EU-retsakter

1. Hvis [...] sektorspecifikke **EU-rets**akter [...] kræver, at væsentlige eller vigtige enheder [...] vedtager foranstaltninger til styring af cybersikkerhedsrisici eller underretter om **væsentlige** hændelser eller [...] cybertrusler, og hvis disse krav har en virkning, der mindst svarer til de forpligtelser, der er fastsat i dette direktiv, finder de relevante bestemmelser i dette direktiv**, herunder bestemmelserne om tilsyn og håndhævelse i kapitel VI,** ikke anvendelse **på sådanne enheder**. **Hvis sektorspecifikke EU-retsakter ikke omfatter alle enheder i en specifik sektor, der falder ind under dette direktivs anvendelsesområde, finder de relevante bestemmelser i dette direktiv fortsat anvendelse på de enheder, der ikke er omfattet af disse sektorspecifikke bestemmelser.**

2. De krav, der er omhandlet i denne artikels stk. 1, anses for at have samme virkning som de forpligtelser, der er fastsat i dette direktiv, hvis den respektive sektorspecifikke EU-retsakt fastsætter øjeblikkelig, i givet fald automatisk og direkte, adgang til underretninger om hændelser fra de kompetente myndigheder i henhold til dette direktiv eller de udpegede CSIRT'er, og hvis:

a) foranstaltningerne til styring af cybersikkerhedsrisici mindst har samme virkning som dem, der er omhandlet i dette direktivs artikel 18, stk. 1 og 2, eller

b) kravene om at underrette om væsentlige hændelser mindst har samme virkning som dem, der er omhandlet i artikel 20, stk. 1-6.

3. Kommissionen gennemgår regelmæssigt anvendelsen af kravene om samme virkning i stk. 1 og 2 i forbindelse med sektorspecifikke bestemmelser i EU-retsakter. Kommissionen hører samarbejdsgruppen og ENISA, når den forbereder disse regelmæssige gennemgange.

Artikel 3

Minimumsharmonisering

Uden at det berører deres øvrige forpligtelser i henhold til EU-retten, kan medlemsstaterne [...] **på de områder, der er omfattet af dette direktiv,** vedtage eller opretholde bestemmelser, der sikrer et højere cybersikkerhedsniveau.

Artikel 4

Definitioner

I dette direktiv forstås ved:

1) "net- og informationssystem":

   a) et elektronisk kommunikationsnet som omhandlet i artikel 2, nr. 1), i direktiv (EU) 2018/1972

   b) enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data

   c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse

2) "sikkerhed i net- og informationssystemer": net- og informationssystemers evne til på et givet sikkerhedsniveau at modstå **begivenheder**, der **kan være [...]** til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller **i forbindelse med** de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer

2a) "elektroniske kommunikationstjenester": elektroniske [...] kommunikationstjenester som omhandlet i artikel 2, nr. 4), i direktiv (EU) 2018/1972

3) "cybersikkerhed": cybersikkerhed som omhandlet i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) 2019/881[33]

4) "national **cybersikkerheds**strategi [...]": en sammenhængende ramme i en medlemsstat, som tilvejebringer en styring med henblik på at opfylde strategiske mål og prioriteter **på området** [...] **cybersikkerhed** [...] i den pågældende medlemsstat

5) "hændelse": enhver begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller de [...] tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare

5a) "omfattende cybersikkerhedshændelse": en hændelse med en væsentlig indvirkning på mindst to medlemsstater, eller hvis forstyrrelse overstiger en medlemsstats evne til at reagere på den

---

[33] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed, om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

6) "håndtering af hændelser": alle handlinger og procedurer, der tager sigte på opdagelse, analyse og inddæmning af og reaktion på en hændelse

6a) "risiko": risikoen for tab eller afbrydelse som følge af en hændelse, udtrykkes som en kombination af omfanget af et sådant tab eller en sådan afbrydelse og sandsynligheden for, at hændelsen indtræffer

7) "cybertrussel": en cybertrussel som omhandlet i artikel 2, nr. 8), i forordning (EU) 2019/881

7**a) "væsentlig cybertrussel": en cybertrussel, som på grundlag af sine tekniske karakteristika kan antages at have potentiale til at få alvorlig indvirkning på en enheds eller dens brugeres net- og informationssystemer ved at forårsage betydelige materielle eller immaterielle tab**

8) "sårbarhed": en svaghed, følsomhed eller fejl i forbindelse med et IKT-aktiv eller et system [...], som kan udnyttes af en cybertrussel

8a) "nærvedhændelse": en begivenhed, der potentielt kunne have forvoldt skade på en enheds eller dens brugeres net- og informationssystemer, men hvor det lykkedes at forhindre, at den indtraf fuldt ud

9) "repræsentant": enhver fysisk eller juridisk person, der er etableret i Unionen, og som udtrykkeligt er udpeget til at handle på vegne af i) en DNS-tjenesteudbyder, en topdomænenavneregistratur (TLD), en udbyder af cloudcomputingtjenester, en datacentertjenesteudbyder, en udbyder af indholdsudsendelsesnetværk som omhandlet i bilag I, punkt 8, eller ii) enheder som omhandlet i bilag II, punkt [...] **6**, der ikke er etableret i Unionen, og som kan kontaktes af en national kompetent myndighed eller en CSIRT i stedet for enheden i forbindelse med forpligtelserne i henhold til dette direktiv

10) "standard": en standard som omhandlet i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012[34]

11) "teknisk specifikation": en teknisk specifikation som omhandlet i artikel 2, nr. 4), i forordning (EU) nr. 1025/2012

12) "internetudvekslingspunkt (IXP)": en netfacilitet, der muliggør sammenkobling af mere end to uafhængige net (autonome systemer), primært med henblik på at lette udvekslingen af internettrafik. Et IXP leverer kun sammenkobling for autonome systemer. Et IXP forudsætter ikke, at internettrafik, som bevæger sig mellem et givet par af deltagende autonome systemer, bevæger sig gennem et tredje autonomt system, og det hverken ændrer eller forstyrrer en sådan trafik

13) "domænenavnesystem (DNS)": et hierarkisk distribueret navngivningssystem, der gør det muligt for slutbrugere at nå frem til tjenester og ressourcer på internettet

14) "DNS-tjenesteudbyder": en enhed, der udbyder rekursive eller autoritative domænenavnsoversættelsestjenester **til** [...] **tredjepartsbrug, med undtagelse af rodnavneservere** [...]

---

[34] Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).

15) "topdomænenavneadministrator": en enhed, der har fået delegeret et specifikt topdomæne, og som er ansvarlig for at administrere topdomænet, herunder registrering af domænenavne under topdomænet og den tekniske drift af topdomænet, herunder drift af dets navneservere, vedligeholdelse af dets databaser og distribution af topdomænezonefiler på navneservere**, idet der ses bort fra situationer, hvor topdomænenavne kun anvendes af en administrator til egen brug**

15a) "enheder, der udbyder domænenavneregistreringstjenester til topdomæner": topdomænenavneadministratorer, registratorer af topdomæner og agenter for registratorer såsom videresælgere og udbydere af proxytjenester

16) "digital tjeneste": en tjeneste som omhandlet i artikel 1, stk. 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535[35]

16a) "tillidstjenester": tillidstjenester som omhandlet i artikel 3, nr. 16), i forordning (EU) nr. 910/2014

---

[35] Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1).

16b) "kvalificeret tillidstjenesteudbyder": en kvalificeret tillidstjenesteudbyder som omhandlet i artikel 3, nr. 20), i forordning (EU) nr. 910/2014

17) "onlinemarkedsplads": en digital tjeneste som omhandlet i artikel 2, litra n), i Europa-Parlamentets og Rådets direktiv 2005/29/EF[36]

18) "onlinesøgemaskine": en digital tjeneste som omhandlet i artikel 2, nr. 5), i Europa-Parlamentets og Rådets forordning (EU) 2019/1150[37]

19) "cloudcomputingtjeneste": en digital tjeneste, som muliggør on demand-administration og giver bred fjernadgang til en skalerbar og elastisk pulje af delbare [...] databehandlingsressourcer**, herunder når disse distribueres i flere områder**

20) "datacentertjeneste": en tjeneste, der omfatter strukturer eller grupper af strukturer, der er dedikeret til central indkvartering, sammenkobling og drift af informationsteknologi og netværksudstyr, der leverer datalagrings-, behandlings- og transporttjenester samt alle faciliteter og infrastrukturer til strømdistribution og miljøkontrol

---

[36] Europa-Parlamentets og Rådets direktiv 2005/29/EF af 11. maj 2005 om virksomheders urimelige handelspraksis over for forbrugerne på det indre marked og om ændring af Rådets direktiv 84/450/EØF og Europa-Parlamentets og Rådets direktiv 97/7/EF, 98/27/EF og 2002/65/EF og Europa-Parlamentets og Rådets forordning (EF) nr. 2006/2004 (direktivet om urimelig handelspraksis) (EUT L 149 af 11.6.2005, s. 22).

[37] Europa-Parlamentets og Rådets forordning (EU) 2019/1150 af 20. juni 2019 om fremme af retfærdighed og gennemsigtighed for brugere af onlineformidlingstjenester (EUT L 186 af 11.7.2019, s. 57).

21) "indholdsleveringsnetværk": et net af geografisk distribuerede servere med henblik på at sikre høj tilgængelighed, adgang til eller hurtig levering af digitalt indhold og digitale tjenester til internetbrugere på vegne af indholds- og tjenesteudbydere

22) "platform for sociale netværkstjenester": en platform, der sætter slutbrugerne i stand til at forbinde, dele, opdage og kommunikere med hinanden på tværs af flere enheder, navnlig via chats, indlæg, videoer og anbefalinger [...]

23) "offentlig forvaltningsenhed": en enhed**, der er anerkendt som sådan i en medlemsstat i overensstemmelse med national ret,** [...] og som opfylder følgende kriterier:

   a) den er oprettet med henblik på at opfylde almennyttige formål og har ikke industriel eller kommerciel karakter

   b) den har status som juridisk person**, eller den er ved lov berettiget til at handle på vegne af en anden enhed med status som juridisk person**

   c) den finansieres for størstedelens vedkommende af staten, en regional myndighed eller af andre offentligretlige organer, eller den er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer, eller den har et administrations-, ledelses- eller tilsynsorgan, hvor mere end halvdelen af medlemmerne udpeges af staten, regionale myndigheder eller andre offentligretlige organer

   d) den har beføjelse til at rette administrative eller lovgivningsmæssige afgørelser til fysiske eller juridiske personer, der påvirker deres rettigheder i forbindelse med grænseoverskridende bevægelighed for personer, varer, tjenesteydelser eller kapital

24) "enhed": enhver fysisk eller juridisk person, der er oprettet og anerkendt som sådan i henhold til den nationale lovgivning på det sted, hvor den er etableret, og som i eget navn kan udøve rettigheder og være underlagt forpligtelser

25) "væsentlig enhed": enhver enhed af en type [...] **som omhandlet i bilag I, og som betegnes som "væsentlig" i overensstemmelse med artikel 2a, stk. 1**

26) "vigtig enhed": enhver enhed af en type [...] **som omhandlet i bilag I og II, og som betegnes som "vigtig" i overensstemmelse med artikel 2a, stk. 2**

26a) "IKT-produkt": et IKT-produkt som omhandlet i artikel 2, nr. 12), i forordning (EU) 2019/881

26aa) "IKT-tjeneste": en IKT-tjeneste som omhandlet i artikel 2, nr. 13), i forordning (EU) 2019/881

26ab) "IKT-proces": en IKT-proces som omhandlet i artikel 2, nr. 14), i forordning (EU) 2019/881

26ac) "udbyder af administrerede tjenester": enhver enhed, der udbyder tjenester såsom net, applikationer, infrastruktur og sikkerhed via løbende og regelmæssig forvaltning, støtte og aktiv administration på kundernes lokaliteter, i deres datacenter for udbydere af administrerede tjenester (hosting) eller i et tredjepartsdatacenter

26ad) "udbyder af administrerede sikkerhedstjenester": enhver enhed, der udbyder outsourcet overvågning og forvaltning af sikkerhedsudstyr og -systemer. Almindelige tjenester omfatter forvaltet firewall, opdagelse af indtrængen, virtuelt privat net, sårbarhedsscanning og antivirustjenester.

Det omfatter også anvendelse af sikkerhedsoperationscentre med stor tilgængelighed (enten fra deres egne faciliteter eller fra andre datacenterudbydere) med henblik på at udbyde tjenester døgnet rundt alle ugens dage, der har til formål at nedbringe det antal operationelle sikkerhedsmedarbejdere, som en virksomhed er nødt til at ansætte, uddanne og fastholde for at opretholde en acceptabel sikkerhedsstatus.

KAPITEL II

Koordinerede lovgivningsmæssige rammer for cybersikkerhed

Artikel 5

National cybersikkerhedsstrategi

1. Hver medlemsstat vedtager en national cybersikkerhedsstrategi, hvori den definerer de strategiske mål og passende politikforanstaltninger og reguleringsmæssige foranstaltninger med henblik på at opnå og opretholde et højt cybersikkerhedsniveau. Den nationale cybersikkerhedsstrategi omfatter navnlig følgende:

   a) [...] mål og prioriteter i medlemsstaternes strategi for cybersikkerhed

   b) en forvaltningsramme med henblik på at nå disse mål og prioriteter, herunder de politikker, der er omhandlet i stk. 2, og rollerne og ansvarsområderne for de forskellige myndigheder og aktører, der deltager i gennemførelsen af strategien [...]

   c) [...] **vejledning** med henblik på at identificere relevante aktiver og **vurdere** cybersikkerhedsrisici i den pågældende medlemsstat [...]

   d) identificering af foranstaltninger, der sikrer beredskab, reaktion og genopretning i forbindelse med hændelser, herunder samarbejde mellem den offentlige og den private sektor

   e) [...]

f) en politikramme for øget koordinering mellem de kompetente myndigheder i henhold til dette direktiv og Europa-Parlamentets og Rådets direktiv (EU) XXXX/XXXX[38] [direktivet om kritiske enheders modstandsdygtighed] med henblik på udveksling af oplysninger om **cybersikkerhedsrisici og** [...] cybertrusler **og -hændelser samt om ikkecyberrisici, -trusler og -hændelser** og udøvelse af tilsynsopgaver**, alt efter hvad der er relevant**

fa) en politikramme for koordinering og samarbejde mellem kompetente myndigheder i henhold til dette direktiv og kompetente myndigheder udpeget i henhold til sektorspecifik lovgivning.

2. Som led i den nationale cybersikkerhedsstrategi vedtager medlemsstaterne navnlig følgende politikker:

a) en politik vedrørende cybersikkerhed i forsyningskæden for IKT-produkter og -tjenester, der anvendes af [...] enheder til levering af deres tjenester

b) **en politik** [...] for medtagelse og specificering af cybersikkerhedsrelaterede krav til IKT-produkter og -tjeneste**r** i forbindelse med offentlige indkøb**, herunder cybersikkerhedscertificering**

c) en politik **for håndtering af sårbarheder, der omfatter fremme og lettelse af** [...] **frivillig** koordineret offentliggørelse af sårbarheder som omhandlet i artikel 6**, stk. 1**

d) en politik vedrørende opretholdelse af den generelle tilgængelighed, [...] integritet **og fortrolighed** i den offentlige centrale del af det åbne internet

e) en politik for fremme og udvikling af **uddannelse,** færdigheder, bevidstgørelse samt forsknings- og udviklingsinitiativer i forbindelse med cybersikkerhed

---

[38] *[Indsæt den fulde titel og EUT-offentliggørelseshenvisning, når den kendes].*

f) en politik for støtte til akademiske institutioner og forskningsinstitutioner med henblik på udvikling af cybersikkerhedsværktøjer og sikker netværksinfrastruktur

g) en politik, relevante procedurer og passende informationsdelingsværktøjer til støtte for frivillig udveksling af cybersikkerhedsoplysninger mellem virksomheder i overensstemmelse med EU-retten

h) en politik, der tilgodeser specifikke behov hos SMV'er, navnlig dem, der er udelukket fra dette direktivs anvendelsesområde, i forbindelse med vejledning og støtte til forbedring af deres modstandsdygtighed over for cyber[...]trusler.

3. Medlemsstaterne underretter Kommissionen om deres nationale cybersikkerhedsstrategier senest tre måneder efter deres vedtagelse. Medlemsstaterne kan **i forbindelse hermed** udelukke **elementer i strategien, der vedrører** [...] national sikkerhed.

4. Medlemsstaterne vurderer deres nationale cybersikkerhedsstrategier regelmæssigt og mindst hvert [...] **femte** år på grundlag af centrale præstationsindikatorer og ændrer dem om nødvendigt. Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) bistår på anmodning **af medlemsstaterne** disse med at udvikle en national strategi og nøgleresultatindikatorer til vurdering af strategien.

Artikel 6

Koordineret offentliggørelse af sårbarheder og et europæisk sårbarhedsregister

1. Hver medlemsstat udpeger en af sine CSIRT'er som omhandlet i artikel 9 som koordinator med henblik på koordineret offentliggørelse af sårbarheder. Den udpegede CSIRT fungerer som betroet formidler og letter om nødvendigt samspillet mellem den underrettende enhed**, den potentielle sårbarhedsejer** og producenten eller udbyderen af IKT-produkter eller -tjenester. **Enhver fysisk eller juridisk person kan, eventuelt anonymt, indberette en sårbarhed som omhandlet i artikel 4, nr. 8), til den udpegede CSIRT. Den udpegede CSIRT sørger for en omhyggelig opfølgning af indberetningen samt fortrolighed af identiteten af den person, der indberetter sårbarheden.** Hvis den indberettede sårbarhed [...] **potentielt kan få væsentlig indvirkning på enheder i mere end én medlemsstat**, samarbejder den udpegede CSIRT for hver berørt medlemsstat**, hvis det er relevant,** med **andre udpegede CSIRT'er i** CSIRT-netværket.

2. ENISA udvikler og vedligeholder et europæisk sårbarhedsregister **i samråd med samarbejdsgruppen**. Med henblik herpå opretter og vedligeholder ENISA passende informationssystemer, -politikker og -procedurer med det formål navnlig at sætte vigtige og væsentlige enheder og deres leverandører af net- og informationssystemer i stand til **frivilligt** at afsløre og registrere **offentligt kendte** sårbarheder i IKT-produkter eller -tjenester samt at give alle interesserede parter adgang til oplysningerne om sårbarheder i registret. Registret skal navnlig indeholde oplysninger, der beskriver sårbarheden, det berørte IKT-produkt eller de berørte IKT-tjenester og alvoren af sårbarheden med hensyn til de omstændigheder, hvorunder den kan udnyttes, tilgængeligheden af relaterede patches og, i mangel af tilgængelige patches, vejledning **udsendt af nationale kompetente myndigheder eller CSIRT'er** til brugere af sårbare produkter og tjenester om, hvordan risiciene som følge af afslørede sårbarheder kan afbødes. **ENISA sørger for, at det europæiske sårbarhedsregister anvender sikker og modstandsdygtig kommunikations- og informationsinfrastruktur.**

Artikel 7

Nationale rammer for styring af cybersikkerhedskriser

1. Hver medlemsstat udpeger en eller flere kompetente myndigheder med ansvar for styring af omfattende **cybersikkerheds**hændelser og -kriser. Medlemsstaterne sikrer, at de kompetente myndigheder har tilstrækkelige ressourcer til på en virkningsfuld og effektiv måde at udføre de opgaver, de pålægges. **Medlemsstaterne sikrer sammenhæng med de eksisterende rammer for generel krisestyring.**

2. Hver medlemsstat identificerer kapaciteter, aktiver og procedurer, der kan indsættes i tilfælde af en krise med henblik på dette direktiv.

3. Hver medlemsstat vedtager en national cybersikkerhedshændelses- og kriseberedskabsplan, hvori der er fastsat mål og nærmere bestemmelser for håndteringen af omfattende cybersikkerhedshændelser og -kriser. Planen skal navnlig indeholde følgende:

   a) målsætninger for nationale beredskabsforanstaltninger og -aktiviteter

   b) de nationale kompetente myndigheders opgaver og ansvarsområder

   c) cybersikkerhedskrisestyringsprocedurer**, herunder deres integration i den generelle nationale krisestyringsramme,** og informationsudvekslingskanaler

   d) beredskabsforanstaltninger, herunder regelmæssige øvelses- og uddannelsesaktiviteter

   e) relevante berørte offentlige og private [...] parter og infrastruktur

   f) nationale procedurer og ordninger mellem relevante nationale myndigheder og organer for at sikre medlemsstatens effektive deltagelse i og støtte til den koordinerede håndtering af omfattende cybersikkerhedshændelser og -kriser på EU-plan.

4. Medlemsstaterne [...] **underretter** Kommissionen **om** udpegelsen af deres kompetente myndigheder, jf. stk. 1, og forelægger **relevante oplysninger vedrørende kravene i stk. 3 om** deres nationale cybersikkerhedshændelses- og cyberkriseberedskabsplaner [...] senest tre måneder efter udpegelsen og vedtagelsen af disse planer. Medlemsstaterne kan udelukke specifikke oplysninger [...], hvis og i det omfang det er [...] nødvendigt af hensyn til deres nationale sikkerhed**, offentlige sikkerhed eller forsvar**.

Artikel 8

Nationale kompetente myndigheder og centrale kontaktpunkter

1. Hver medlemsstat udpeger en eller flere kompetente myndigheder med ansvar for cybersikkerhed og for de tilsynsopgaver, der er omhandlet i kapitel VI i dette direktiv. Medlemsstaterne kan tildele en eller flere eksisterende myndigheder denne rolle.

2. De i stk. 1 omhandlede kompetente myndigheder fører tilsyn med anvendelsen af dette direktiv på nationalt plan.

3. Hver medlemsstat udpeger et nationalt centralt kontaktpunkt for cybersikkerhed ("centralt kontaktpunkt"). Hvis en medlemsstat kun udpeger én kompetent myndighed, fungerer denne kompetente myndighed ligeledes som det centrale kontaktpunkt for den pågældende medlemsstat.

4. Hvert centralt kontaktpunkt udøver en forbindelsesfunktion for at sikre grænseoverskridende samarbejde mellem dets medlemsstats myndigheder og de relevante myndigheder i andre medlemsstater samt for at sikre tværsektorielt samarbejde med andre nationale kompetente myndigheder i dets medlemsstat.

5. Medlemsstaterne sikrer, at de i stk. 1 omhandlede kompetente myndigheder og de centrale kontaktpunkter har tilstrækkelige ressourcer til på en effektiv måde at udføre de opgaver, som de pålægges, og dermed opfylde målene i dette direktiv. Medlemsstaterne sikrer et effektivt, virkningsfuldt og sikkert samarbejde mellem de udpegede repræsentanter i den i artikel 12 omhandlede samarbejdsgruppe.

6. Hver medlemsstat underretter uden unødig forsinkelse Kommissionen om udpegelsen af den i stk. 1 omhandlede kompetente myndighed og det i stk. 3 omhandlede centrale kontaktpunkt, deres opgaver og enhver senere ændring heraf. Hver medlemsstat offentliggør udpegelsen af disse. Kommissionen offentliggør listen over udpegede centrale kontaktpunkter.

Artikel 9

Enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)

1. Hver medlemsstat udpeger en eller flere CSIRT'er, der skal opfylde kravene i artikel 10, stk. 1, som mindst omfatter de i bilag I og II omhandlede sektorer, delsektorer eller enheder, og som er ansvarlige for at håndtere hændelser og risici i overensstemmelse med en nøje fastlagt proces. En CSIRT kan oprettes inden for en kompetent myndighed, jf. artikel 8.

2. Medlemsstaterne sikrer, at hver CSIRT har tilstrækkelige ressourcer til at udføre sine opgaver som fastsat i artikel 10, stk. 2, effektivt. **CSIRT'er kan ved udførelsen af disse opgaver prioritere ydelse af særlige tjenester til enheder på grundlag af en risikobaseret tilgang.**

3. Medlemsstaterne sikrer, at hver CSIRT råder over en passende, sikker og modstandsdygtig kommunikations- og informationsinfrastruktur til udveksling af oplysninger med væsentlige og vigtige enheder og andre relevante interesserede parter. Med henblik herpå sikrer medlemsstaterne, at CSIRT'erne bidrager til udbredelsen af sikre informationsudvekslingsværktøjer.

4. CSIRT'er samarbejder og udveksler, hvor det er relevant, relevante oplysninger i overensstemmelse med artikel 26 med pålidelige sektorfællesskaber eller tværsektorielle fællesskaber af væsentlige og vigtige enheder.

5. CSIRT'er deltager i peer[...]**læring**, der tilrettelægges i overensstemmelse med artikel 16.

6. Medlemsstaterne sikrer et effektivt og sikkert samarbejde mellem deres CSIRT'er i det i artikel 13 omhandlede CSIRT-netværk.

7. Medlemsstaterne underretter uden unødig forsinkelse Kommissionen om de CSIRT'er, der er udpeget i henhold til stk. 1, den CSIRT-koordinator, der er udpeget i henhold til artikel 6, stk. 1, og deres respektive opgaver i relation til de i bilag I og II omhandlede enheder.

8. Medlemsstaterne kan anmode ENISA om bistand til at udvikle nationale CSIRT'er.

Artikel 10

Krav til CSIRT'er og deres opgaver

1. CSIRT'er skal opfylde nedenstående krav:

   a) CSIRT'er skal sikre et højt tilgængelighedsniveau for deres kommunikations[...]**kanaler** ved at undgå svage punkter ("single points of failure") og ved til enhver tid at have flere muligheder for at blive kontaktet og for at kontakte andre. CSIRT'er skal tydeligt angive kommunikationskanalerne og gøre dem kendt af samarbejdspartnere.

   b) CSIRT'ers lokaler og de underliggende informationssystemer skal være placeret i sikrede områder.

c) CSIRT'er skal være udstyret med et passende system til administration og videresendelse af anmodninger med henblik på at lette effektive overdragelser.

d) CSIRT'er skal have tilstrækkeligt personale til at sikre tilgængelighed døgnet rundt.

e) CSIRT'er skal være udstyret med redundante systemer og backup-arbejdsplads for at sikre kontinuiteten i deres tjenester.

f) CSIRT'er skal have mulighed for at deltage i internationale samarbejdsnetværk.

2. CSIRT'er har følgende opgaver:

a) overvågning af cybertrusler, -sårbarheder og -hændelser på nationalt plan

b) tidlig varsling, alarmer, meddelelser og formidling af oplysninger til væsentlige og vigtige enheder samt til **kompetente myndigheder og** andre relevante interesserede parter om cybertrusler, -sårbarheder og -hændelser

c) reaktion på hændelser

d) indsamling og analyse af kriminaltekniske data og udarbejdelse af dynamiske risiko- og hændelsesanalyser og situationsbevidsthed vedrørende cybersikkerhed

e) **[...]** gennemførelse af en proaktiv scanning af net- og informationssystemer [...] **for at opdage sårbarheder med potentiel væsentlig indvirkning, forudsat at der ikke trænges ind i net- og informationssystemerne, hvis der ikke foreligger samtykke fra den pågældende enhed, og at deres funktion ikke påvirkes negativt**

f) deltagelse i CSIRT-netværket og ydelse af gensidig bistand **i overensstemmelse med deres kapacitet og kompetencer** til andre medlemmer af netværket efter anmodning fra disse

fa) hvor det er relevant, funktion som koordinator med henblik på processen for koordineret offentliggørelse af sårbarheder i medfør af artikel 6, stk. 1, som navnlig skal omfatte lettelse af samspillet mellem de underrettende enheder, den potentielle sårbarhedsejer og producenten eller udbyderen af IKT-produkter eller -tjenester i tilfælde, hvor det er nødvendigt, identificere og kontakte berørte enheder, støtte underrettende enheder, forhandle tidsfrister for offentliggørelse og håndtering af sårbarheder, der påvirker flere organisationer (koordineret offentliggørelse af sårbarheder med flere parter).

3. CSIRT'er etablerer samarbejdsrelationer med relevante aktører i den private sektor med henblik på bedre at nå direktivets mål.

3a. CSIRT'er kan etablere samarbejdsforbindelser med tredjelandes nationale CSIRT'er. Som led i et sådant samarbejde kan de udveksle relevante oplysninger, herunder personoplysninger, i overensstemmelse med EU-retten om databeskyttelse.

4. For at lette samarbejdet fremmer CSIRT'er vedtagelse og anvendelse af fælles eller standardiseret praksis, klassifikationsordninger og taksonomier i forbindelse med følgende:

a) procedurer for håndtering af hændelser

b) krisestyring på cybersikkerhedsområdet

c) koordineret offentliggørelse af sårbarheder.

Artikel 11

Samarbejde på nationalt plan

1. Hvis en medlemsstats kompetente myndigheder som omhandlet i artikel 8, det centrale kontaktpunkt og CSIRT('er) er adskilte enheder, samarbejder de med hensyn til opfyldelsen af de forpligtelser, der er fastlagt i dette direktiv.

2. Medlemsstaterne sikrer, at enten deres kompetente myndigheder eller deres CSIRT'er modtager meddelelser om hændelser og væsentlige cybertrusler og nærvedhændelser, som indgives i henhold til dette direktiv. Hvis en medlemsstat beslutter, at dens CSIRT'er ikke skal modtage disse underretninger, skal CSIRT'erne, i det omfang det er nødvendigt for udførelsen af deres opgaver, have adgang til data om hændelser, som de væsentlige eller vigtige enheder har meddelt i henhold til artikel 20.

3. Hver medlemsstat sikrer, at dens kompetente myndigheder eller CSIRT'er underretter dens centrale kontaktpunkt om underretninger om hændelser, væsentlige cybertrusler og nærvedhændelser, som indgives i henhold til dette direktiv.

4. I det omfang det er nødvendigt for effektivt at udføre de opgaver og forpligtelser, der er fastsat i dette direktiv, sikrer medlemsstaterne et passende samarbejde mellem de kompetente myndigheder, **CSIRT'er,** de centrale kontaktpunkter samt de retshåndhævende myndigheder, databeskyttelsesmyndigheder og de **kompetente** myndigheder**, der er udpeget** [...] i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed] [...], **de kompetente myndigheder i henhold til Kommissionens gennemførelsesforordning (EU) 2019/1583, de nationale tilsynsmyndigheder, der er udpeget i overensstemmelse med direktiv (EU) 2018/1972, de nationale myndigheder, der er udpeget i medfør af artikel 17 i forordning (EU) nr. 910/2014,** [...] de nationale finansmyndigheder, der er udpeget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) XXXX/XXXX [DORA-forordningen]**, samt kompetente myndigheder udpeget i henhold til andre sektorspecifikke EU-retsakter** i den pågældende medlemsstat.

5. Medlemsstaterne sikrer, at deres kompetente myndigheder **i henhold til dette direktiv og de kompetente myndigheder, der er udpeget i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed]**, regelmæssigt **udveksler** [...] oplysninger [...] om **identifikation af kritiske enheder,** cybersikkerhedsrisici og cyber**trusler og -hændelser samt om ikkecyberrisici, -trusler og -hændelser**, som påvirker væsentlige enheder, der er identificeret som kritiske **[**eller som enheder, der svarer til kritiske enheder,**]** i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed] samt de foranstaltninger, der træffes [...] som reaktion på disse risici og hændelser. **Medlemsstaterne sikrer også, at kompetente myndigheder i henhold til dette direktiv** [...] **og de kompetente myndigheder, der er udpeget i henhold til forordning (EU) XXXX/XXXX [DORA-forordningen], direktiv (EU) 2018/1972 og forordning (EU) nr. 910/2014, regelmæssigt udveksler relevante oplysninger.**

For så vidt angår tillidstjenesteudbydere og [...] navnlig [...] i tilfælde, hvor denne tilsynsrolle i henhold til dette direktiv tildeles et andet organ end de tilsynsorganer, der er udpeget i medfør af forordning (EU) nr. 910/2014, samarbejder de nationale kompetente myndigheder i henhold til dette direktiv rettidigt tæt med hinanden ved at udveksle relevante oplysninger for at sikre et effektivt tilsyn og tillidstjenesteudbyderes opfyldelse af kravene i dette direktiv og forordning [XXXX/XXXX], **og den nationale kompetente myndighed i henhold til dette direktiv underretter, hvis det er relevant, uden unødig forsinkelse eIDAS-tilsynsorganet om enhver underretning om væsentlige cybertrusler eller -hændelser med indvirkning på tillidstjenester.**

5a. **Med henblik på [...] at forenkle rapportering af hændelser kan medlemsstaterne oprette et centralt kontaktpunkt for alle meddelelser, der kræves i henhold til dette direktiv samt i henhold til forordning (EU) 2016/679 og direktiv 2002/58/EF, alt efter tilfældet. Medlemsstaterne kan anvende det centrale kontaktpunkt for underretninger, der kræves i henhold til andre sektorspecifikke EU-retsakter. Dette centrale kontaktpunkt berører ikke anvendelsen af bestemmelserne i forordning (EU) 2016/679 og direktiv 2002/58/EF, navnlig bestemmelserne om uafhængige tilsynsmyndigheder.**

KAPITEL III

EU*-samarbejde*

Artikel 12

Samarbejdsgruppe

1. For at støtte og lette det strategiske samarbejde og udvekslingen af oplysninger mellem medlemsstaterne **samt** [...] **for at styrke tilliden og fortroligheden** [...] nedsættes der en samarbejdsgruppe.

2. Samarbejdsgruppen udfører sine opgaver på grundlag af toårige arbejdsprogrammer som omhandlet i stk. 6.

3. Samarbejdsgruppen består af repræsentanter fra medlemsstaterne, Kommissionen og ENISA. Tjenesten for EU's Optræden Udadtil deltager som observatør i samarbejdsgruppens aktiviteter. De europæiske tilsynsmyndigheder (ESA'er) **og de kompetente myndigheder, der er udpeget i henhold til forordning (EU) XXXX/XXXX [DORA-forordningen],** [...] kan deltage i samarbejdsgruppens aktiviteter **i overensstemmelse med artikel 42, stk. 1, i forordning (EU) XXXX/XXXX [DORA-forordningen]**.

   Samarbejdsgruppen kan, hvis det er relevant, indbyde repræsentanter fra relevante interessenter til at deltage i arbejdet.

   Sekretariatsopgaverne varetages af Kommissionen.

4. Samarbejdsgruppen har følgende opgaver:

   a) at vejlede de kompetente myndigheder i forbindelse med omsætningen og gennemførelsen af dette direktiv

   aa) at yde vejledning i udarbejdelse og gennemførelse af politikker for koordineret offentliggørelse af sårbarheder, jf. artikel 5, stk. 2, litra c), og artikel 6, stk. 1

b) at udveksle bedste praksis og oplysninger i forbindelse med gennemførelsen af dette direktiv, herunder i forbindelse med cybertrusler, -hændelser og -sårbarheder, nærvedhændelser, bevidstgørelsesinitiativer, uddannelse, øvelser og færdigheder, opbygning af kapacitet samt standarder og tekniske specifikationer

c) at udveksle rådgivning og samarbejde med Kommissionen om nye politiske initiativer inden for cybersikkerhed

d) at udveksle rådgivning og samarbejde med Kommissionen om udkast til Kommissionens gennemførelsesretsakter [...] vedtaget i henhold til dette direktiv

e) at udveksle bedste praksis og oplysninger med relevante EU-institutioner, -organer, -kontorer og -agenturer

ea) at udveksle synspunkter om gennemførelsen af sektorspecifik lovgivning med cybersikkerhedsaspekter

f) at rådgive om den i artikel 16, stk. 7, omhandlede peer[...]**læring**

g) at drøfte **erfaringerne** [...] fra fælles tilsynsaktiviteter i grænseoverskridende sager, jf. artikel 34

h) at yde strategisk vejledning til CSIRT-netværket **og EU–CyCLONe** om specifikke nye spørgsmål

ha) at udveksle synspunkter om politisk opfølgning af omfattende cybersikkerhedshændelser på grundlag af erfaringerne fra CSIRT-netværket og EU-CyCLONe

i) at bidrage til cybersikkerhedskapaciteter i hele Unionen ved at lette udvekslingen af nationale embedsmænd gennem et kapacitetsopbygningsprogram, der omfatter personale fra medlemsstaternes kompetente myndigheder eller CSIRT'er

j) at tilrettelægge regelmæssige fælles møder med relevante private interesserede parter fra hele Unionen for at drøfte gruppens aktiviteter og indsamle input om nye politiske udfordringer

k) at drøfte det arbejde, der er udført i forbindelse med cybersikkerhedsøvelser, herunder ENISA's arbejde

ka) at etablere peerlæringsmekanismen i overensstemmelse med dette direktivs artikel 16

5. Samarbejdsgruppen kan anmode CSIRT-netværket om en teknisk rapport om udvalgte emner.

6. Senest … [24 måneder efter datoen for dette direktivs ikrafttræden] og derefter hvert andet år udarbejder samarbejdsgruppen et arbejdsprogram for de foranstaltninger, der skal iværksættes for at gennemføre dens mål og opgaver. Tidsrammen for det første program, der vedtages i henhold til dette direktiv, tilpasses tidsrammen for det sidste program, der er vedtaget i henhold til direktiv (EU) 2016/1148.

7. Kommissionen vedtager gennemførelsesretsakter, hvori der fastlægges proceduremæssige ordninger, som er nødvendige for samarbejdsgruppens funktion. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 37, stk. 2.

8. Samarbejdsgruppen mødes regelmæssigt og mindst en gang om året med gruppen for kritiske enheders modstandsdygtighed, der er nedsat i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed] for at fremme strategisk samarbejde og **lette** udveksling af oplysninger.

Artikel 13

CSIRT-netværket

1. Med henblik på at bidrage til skabelse af tillid mellem medlemsstaterne og fremme et hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne oprettes der et netværk af nationale CSIRT'er.

2. CSIRT-netværket består af repræsentanter fra medlemsstaternes CSIRT'er, **der er udpeget i overensstemmelse med artikel 9**, og CERT-EU. Kommissionen deltager i CSIRT-netværket som observatør. ENISA varetager sekretariatsopgaverne og støtter aktivt samarbejdet mellem CSIRT'erne.

3. CSIRT-netværket har følgende opgaver:

   a) at udveksle oplysninger om CSIRT'ers kapaciteter

   b) at udveksle relevante oplysninger om hændelser, nærvedhændelser, cybertrusler, -risici og -sårbarheder

ba) **at udveksle oplysninger vedrørende cybersikkerhedspublikationer og -henstillinger**

bb) **at dele tekniske løsninger, der letter den tekniske håndtering af hændelser**

bc) **at udveksle bedste praksis, værktøjer og processer vedrørende CSIRT'ernes opgaver**

c) efter anmodning fra et [...] **medlem** af CSIRT-netværket, der potentielt er berørt af en hændelse, at udveksle og drøfte oplysninger i forbindelse med denne hændelse og tilknyttede cybertrusler, -risici og -sårbarheder

d) på anmodning af et [...] **medlem** af CSIRT-netværket at drøfte og, når det er muligt, gennemføre en samordnet reaktion på en hændelse, som er identificeret inden for den medlemsstats jurisdiktion

e) at yde medlemsstaterne støtte til håndtering af grænseoverskridende hændelser i henhold til dette direktiv

f) at samarbejde**, udveksle bedste praksis** og yde bistand til udpegede CSIRT'er, jf. artikel 6, med hensyn til forvaltning af [...] koordineret offentliggørelse af sårbarheder, der berører flere producenter eller udbydere af IKT-produkter, -tjenester og -processer, som er etableret i forskellige medlemsstater

g) at drøfte og identificere yderligere former for operationelt samarbejde, herunder i forhold til:

    i) kategorier af cybertrusler og -hændelser

    ii) tidlig varsling

    iii) gensidig bistand

iv) principper og retningslinjer for koordination som reaktion på grænseoverskridende risici og hændelser

v) bidrag til den nationale cybersikkerhedshændelses- og kriseberedskabsplan, der er omhandlet i artikel 7, stk. 3, **efter anmodning fra en medlemsstat**

h) at oplyse samarbejdsgruppen om sine aktiviteter og om yderligere former for operationelt samarbejde, som drøftes i henhold til litra g), **og**, hvis det er nødvendigt, anmode om vejledning i forbindelse hermed

i) at gøre status over cybersikkerhedsøvelser, herunder fra dem, der tilrettelægges af ENISA

j) på anmodning af en given CSIRT at drøfte denne CSIRT's kapaciteter og beredskab

k) at samarbejde og udveksle oplysninger med regionale sikkerhedsoperationscentre og EU-sikkerhedsoperationscentre for at forbedre den fælles situationsbevidsthed om hændelser og trusler i hele Unionen

l) at drøfte den i artikel 16, stk. 7, omhandlede peer[...]**læring**

m) at udstede retningslinjer for at lette konvergensen mellem operationel praksis med hensyn til anvendelsen af bestemmelserne i denne artikel vedrørende operationelt samarbejde.

4. Med henblik på den i artikel 35 omhandlede evaluering og senest [24 måneder efter datoen for dette direktivs ikrafttræden] og derefter hvert andet år vurderer CSIRT-netværket de fremskridt, der er gjort med det operationelle samarbejde, og udarbejder en rapport. Rapporten skal navnlig drage konklusioner om resultaterne af den i artikel 16 omhandlede peer**læring**, [...] som er gennemført vedrørende nationale CSIRT'er, herunder konklusioner og henstillinger, der forfølges i henhold til denne artikel. Rapporten forelægges ligeledes for samarbejdsgruppen.

5. CSIRT-netværket vedtager sin egen forretningsorden.

6. CSIRT-netværket samarbejder med EU-CyCLONe på grundlag af aftalte proceduremæssige ordninger.

Artikel 14

Det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe)

1. For at støtte den koordinerede forvaltning af omfattende cybersikkerhedshændelser og -kriser på operationelt plan og sikre regelmæssig udveksling af oplysninger mellem medlemsstaterne og Unionens institutioner, organer og agenturer oprettes hermed det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe).

2. EU-CyCLONe består af repræsentanter for medlemsstaternes **cyber**krisestyringsmyndigheder, der er udpeget i overensstemmelse med artikel 7 [...]. **Kommissionen deltager i netværkets aktiviteter som observatør.** ENISA varetager netværkets sekretariatsfunktion og støtter en sikker udveksling af oplysninger **samt udbyder de nødvendige værktøjer til at støtte samarbejdet mellem medlemsstaterne, så der sørges for en sikker udveksling af oplysninger.**

   EU-CyCLONe kan, hvis det er relevant, indbyde repræsentanter fra relevante interessenter til at deltage i arbejdet.

3. EU-CyCLONe har til opgave at

   a) øge beredskabet i forbindelse med håndtering af væsentlige cybersikkerheds[...]hændelser og -kriser

   b) udvikle en fælles situationsbevidsthed [...] i forbindelse med væsentlige cybersikkerheds[...]hændelser og -kriser

   ba) vurdere konsekvenserne og virkningen af relevante væsentlige cybersikkerhedshændelser og foreslå mulige afbødende foranstaltninger

   c) koordinere **styringen af** væsentlige cybersikkerhedshændelser og -kriser [...] og støtte beslutningstagning på politisk plan i forbindelse med sådanne hændelser og kriser

   d) drøfte sine nationale planer for cybersikkerhedshændelser og **-krise**beredskabsplaner **efter anmodning fra en medlemsstat**, jf. artikel 7, stk. **3**[...][...]

4. EU-CyCLONe vedtager selv sin forretningsorden.

5. EU-CyCLONe aflægger regelmæssigt rapport til samarbejdsgruppen om **forvaltningen af væsentlige cybersikkerhedshændelser og -kriser** [...] med særligt fokus på deres indvirkning på væsentlige og vigtige enheder.

6. EU-CyCLONe samarbejder med CSIRT-netværket på grundlag af aftalte proceduremæssige ordninger.

7. EU-CyCLONe forelægger Europa-Parlamentet og Rådet en rapport med en vurdering af sit arbejde senest [24 måneder efter datoen for dette direktivs ikrafttræden].

Artikel 14a

Internationalt samarbejde

Unionen kan, hvor det er relevant, i overensstemmelse med artikel 218 i TEUF indgå internationale aftaler med tredjelande eller internationale organisationer, som giver disse mulighed for og tilrettelægger deres deltagelse i nogle af samarbejdsgruppens aktiviteter, CSIRT-netværket og EU-CyCLONe, i overensstemmelse med EU-retten om databeskyttelse.

Artikel 15

Rapport om cybersikkerhedssituationen i Unionen

1. ENISA udarbejder i samarbejde med Kommissionen **og samarbejdsgruppen** hvert andet år en rapport om cybersikkerhedssituationen i Unionen. **Navnlig**[...] skal rapporten [...] indeholde [...] følgende:

   aa) **en cybersikkerhedsrisikovurdering på EU-plan, der tager trusselsbilledet i betragtning**

   a) [...] **en vurdering af** udviklingen af cybersikkerhedskapaciteter i den offentlige og den private sektor i hele Unionen

   b) [...]

   c) **en samlet vurdering på grundlag af kvantitative og kvalitative** cybersikkerheds**indikatorer,** der giver et [...] **overblik** over cybersikkerhedskapaciteternes modenhedsniveau**, herunder sektorspecifikke kapaciteter**.

2. Rapporten skal indeholde særlige politiske henstillinger med henblik på at øge cybersikkerhedsniveauet i hele Unionen og et sammendrag af resultaterne for den pågældende periode fra agenturets tekniske EU-cybersikkerhedsrapport, som udsendes af ENISA i overensstemmelse med artikel 7, stk. 6, i forordning (EU) 2019/881.

Artikel 16

Peerlæring

1. **Med henblik på at styrke den gensidige tillid, opnå et højt fælles cybersikkerhedsniveau og styrke medlemsstaternes cybersikkerhedskapaciteter og -politikker, som er nødvendige for effektivt at gennemføre dette direktiv** [...] fastlægger **samarbejdsgruppen** [...] **med støtte fra Kommissionen og** efter høring af [...] ENISA **og, hvis det er relevant, CSIRT-netværket** og senest **24 [...]** måneder efter dette direktivs ikrafttræden metoden [...] **til et objektivt, ikkediskriminerende og retfærdigt** peer**lærings**system [...] **vedrørende** medlemsstaternes [...] **gennemførelse af dette direktiv**. **Deltagelse i peerlæringen er frivillig. Systemet består af vurderingsrunder**[...], der foretages af cybersikkerhedseksperter fra andre medlemsstater [...] og omfatter [...] **en eller flere af** følgende **aspekter**:

   i) [...] gennemførelsen af de krav til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, der er omhandlet i artikel 18 og 20

   ii) kapaciteten [...], herunder de [...] ressourcer, der er til rådighed, og [...] de nationale kompetente myndigheders varetagelse af deres opgaver**, der er omhandlet i artikel 8, og CSIRT'er, der er omhandlet i artikel 9**

[...]

iii[...]) [...] **gennemførelsen** af gensidig bistand, jf. artikel 34

iv) [...] **gennemførelsen** af den ramme for informationsudveksling, der er omhandlet i artikel 26 [...].

2. **De kriterier, på grundlag af hvilke medlemsstaterne skal udpege eksperter, der er kvalificerede til at deltage i peerlæringsrunderne, skal være** [...] objektive, ikkediskriminerende, retfærdige og gennemsigtige [...] **og skal være indeholdt i den i stk. 1 omhandlede metode**. ENISA og Kommissionen [...] **kan** udpege eksperter, der deltager som observatører i [...] **peerlæringsrunder**. [...]

3. [...] .

3a. Inden peerlæringsrunderne påbegyndes, kan medlemsstaterne foretage en selvevaluering af de aspekter, der er omfattet af den pågældende peerlæringsrunde, og udlevere denne selvevaluering til de udpegede eksperter, der er omhandlet i stk. 2.

4. Peer[...]**læring** [...] **kan** omfatte [...] **fysiske** eller virtuelle besøg på stedet og udvekslinger uden for stedet. I henhold til princippet om godt samarbejde giver de medlemsstater, [...] **der deltager i peerlæringen** de udpegede eksperter de [...] oplysninger, som er nødvendige for vurderingen [...]**, med forbehold af national ret eller EU-retten vedrørende beskyttelse af fortrolige eller klassificerede informationer eller for at varetage væsentlige statslige funktioner, f.eks. den nationale sikkerhed.** Alle oplysninger, der indhentes i forbindelse med peer[...]**læring**sprocessen, anvendes kun til dette formål. De eksperter, der deltager i peer[...]**læringen**, må ikke videregive følsomme eller fortrolige oplysninger, som er indhentet i [...] **den forbindelse** til tredjemand. **Den medlemsstat, der deltager i peerlæringen, kan gøre indsigelse mod udpegelsen af bestemte eksperter af behørigt begrundede årsager, der meddeles samarbejdsgruppen.**

5. Når **de har været underkastet en peerlæringsrunde** [...], må de samme aspekter ikke underkastes yderligere peer[...]**læringsrunder** [...] **for de deltagende** medlemsstate**r** i de [...] **fire** år, der følger efter afslutningen af **nævnte** [...] peer[...]**læringsrunde**, **medmindre den pågældende medlemsstat anmoder om det eller aftaler det efter forslag** [...] fra **samarbejdsgruppen[...]**.

6. [...]

7. Eksperter, der deltager i peer[...]**læringsrunder**, udarbejder rapporter om resultaterne og konklusionerne af [...] **vurderingerne**. **Medlemsstaterne har mulighed for at fremsætte bemærkninger til deres respektive udkast til rapporterne, som vedlægges rapporten.** De **endelige** rapporter forelægges for [...] samarbejdsgruppen [...]. **Medlemsstaterne kan beslutte at gøre deres respektive rapporter offentligt tilgængelige.**

KAPITEL IV

Forpligtelser vedrørende styring og rapportering af cybersikkerhedsrisici

AFDELING I

Styring og rapportering af cybersikkerhedsrisici

Artikel 17

Forvaltning

1. Medlemsstaterne sikrer, at ledelsesorganerne for væsentlige og vigtige enheder godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 18, [...] **fører tilsyn** med dens gennemførelse og [...] **kan gøres** ansvarlige for enhedernes manglende overholdelse af forpligtelserne i henhold til denne artikel.

   Anvendelsen af dette stykke berører ikke medlemsstatens nationale ret for så vidt angår regler om ansvar i offentlige institutioner samt offentligt ansattes og valgte og udpegede tjenestemænds ansvar.

2. Medlemsstaterne sikrer, at **medlemmerne af ledelsesorganet** [...] regelmæssigt **skal** følge [...] kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici og styringspraksisser samt deres indvirkning på enhedens drift.

Artikel 18

Foranstaltninger til styring af cybersikkerhedsrisici

1**a.** **Dette direktiv anvender en tilgang, der omfatter alle risici, som omfatter beskyttelse af net- og informationssystemer og deres fysiske miljø mod begivenheder, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller i forbindelse med de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer.**

1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder [...] træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- [...] og informationssystemer, som disse enheder anvender til at levere deres tjenester. Under hensyntagen til deres aktuelle tekniske niveau **og implementeringsomkostninger** skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen. **Ved vurderingen af disse foranstaltningers proportionalitet tages der behørigt hensyn til graden af enhedens eksponering for risici, dens størrelse, sandsynligheden for, at der indtræffer hændelser, og til, hvor alvorlige de er. Under hensyntagen til omfanget og typen af risiko for samfundet i tilfælde af hændelser, der påvirker væsentlige eller vigtige enheder, kan de foranstaltninger til styring af cybersikkerhedsrisici, der pålægges vigtige enheder, være lempeligere end dem, der pålægges væsentlige enheder.**

2. De i stk. 1 omhandlede foranstaltninger omfatter mindst følgende:

a) politikker for risikoanalyse og informationssystemsikkerhed

b) håndtering af hændelser (forebyggelse, opdagelse, [...] reaktion på **og genopretning efter** [...] hændelser)

c) driftskontinuitet og krisestyring

d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forbindelserne mellem den enkelte enhed og dens **direkte** leverandører eller tjenesteydere såsom leverandører af datalagrings- og databehandlingstjenester eller administrerede sikkerhedstjenester

e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

f) politikker og procedurer [...] til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici

g) **politik om** brug af kryptografi og kryptering

ga) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.

3. Medlemsstaterne sikrer, at enheder, når de overvejer passende foranstaltninger som omhandlet i stk. 2, litra d), [...] **skal** tage hensyn til de sårbarheder, der er specifikke for hver **direkte** leverandør og tjenesteudbyder, og den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. **Medlemsstaterne sikrer også, at enhederne, når de overvejer passende foranstaltninger som omhandlet i stk. 2, litra d), skal tage hensyn til resultaterne af de koordinerede risikovurderinger, der er foretaget i overensstemmelse med artikel 19, stk. 1.**

4. Medlemsstaterne sikrer, at hvis en enhed finder, at dens tjenester eller opgaver ikke er i overensstemmelse med kravene i stk. 2, træffer den uden unødig forsinkelse alle nødvendige korrigerende foranstaltninger for at bringe den pågældende tjeneste i overensstemmelse med kravene.

5. Kommissionen kan vedtage gennemførelsesretsakter med henblik på at fastlægge de tekniske og metodiske specifikationer **samt, om nødvendigt, sektorspecifikke særtræk** for de i **denne artikels** stk. 2 omhandlede elementer. **Senest [18 måneder efter dette direktivs ikrafttræden] vedtager Kommissionen gennemførelsesretsakter med henblik på at fastlægge de tekniske og metodiske specifikationer for de enheder, der er omhandlet i artikel 24, stk. 1, og de tillidstjenesteudbydere, der er omhandlet i punkt 8 i bilag I.Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 37, stk. 2.** Når[...] Kommissionen udarbejder [...] **sådanne gennemførelses** retsakter **følger** den [...] i videst muligt omfang internationale og europæiske standarder samt relevante tekniske specifikationer **og udveksler rådgivning med samarbejdsgruppen og ENISA om udkastet til gennemførelsesretsakt i overensstemmelse med artikel 12, stk. 4, litra d).**

6. [...]

Artikel 19

Koordinerede EU-risikovurderinger af kritiske forsyningskæder

1. Samarbejdsgruppen kan i samarbejde med Kommissionen og ENISA foretage koordinerede sikkerhedsrisikovurderinger af specifikke kritiske IKT-tjenester, -systemer eller -produktforsyningskæder under hensyntagen til tekniske og, hvor det er relevant, ikketekniske risikofaktorer.

2. Kommissionen identificerer efter høring af samarbejdsgruppen og ENISA de specifikke kritiske IKT-tjenester, -systemer eller -produkter, der kan være genstand for den i stk. 1 omhandlede koordinerede risikovurdering.

Artikel 20

Rapporteringsforpligtelser

1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder uden unødig forsinkelse underretter de kompetente myndigheder eller CSIRT'en i overensstemmelse med stk. 3 og 4 om enhver hændelse, der har en væsentlig indvirkning på leveringen af deres tjenester. Hvor det er relevant, underretter disse enheder uden unødig forsinkelse modtagerne af deres tjenester om **disse** hændelser, der kan forventes at påvirke leveringen af den pågældende tjeneste negativt. Medlemsstater sikrer, at disse enheder bl.a. indberetter alle oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT'en at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen. **Selve underretningen medfører ikke et øget ansvar for den underrettende enhed.**

2. [...]

Hvor det er relevant, underretter [...]**de væsentlige og vigtige** enheder uden unødig forsinkelse modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller afhjælpende foranstaltninger, som disse modtagere kan træffe som reaktion på denne trussel. Hvis det er relevant, underretter enhederne også disse modtagere om selve truslen. **Selve** underretningen medfører ikke et øget ansvar for den underrettende enhed.

3. En hændelse anses for at være væsentlig, hvis:

   a) hændelsen har forårsaget eller potentielt kan forårsage **alvorlige** [...] driftsforstyrrelser **i tjenesten** eller økonomiske tab for den pågældende enhed

   b) hændelsen har påvirket eller kan påvirke andre fysiske eller juridiske personer ved at forårsage betydelige materielle eller immaterielle tab.

4. Medlemsstaterne sikrer, at de berørte enheder med henblik på den i stk. 1 omhandlede underretning fremsender følgende til de kompetente myndigheder eller CSIRT'en:

   a) uden unødig forsinkelse og under alle omstændigheder inden for 24 timer efter at have fået kendskab til hændelsen en indledende underretning **som en tidlig varsling**, som, hvis det er relevant, skal angive, om hændelsen formodes at være forårsaget af ulovlige eller ondsindede handlinger

   b) efter anmodning fra en kompetent myndighed eller en CSIRT, en foreløbig rapport om relevante statusopdateringer

   c) en **endelig** rapport senest en måned efter forelæggelsen af den i litra a) omhandlede [...] **indledende underretning**, der som minimum omfatter følgende:

      i) en detaljeret beskrivelse af hændelsen, dens alvorlighed og indvirkning

      ii) den type trussel eller grundlæggende årsag, der sandsynligvis udløste hændelsen

      iii) anvendte og igangværende afbødende foranstaltninger.

   Medlemsstaterne fastsætter bestemmelser om, at den pågældende enhed i behørigt begrundede tilfælde og efter aftale med de kompetente myndigheder eller CSIRT'en kan fravige de frister, der er fastsat i litra a) og c). **Navnlig kan en fravigelse fra den frist, der er omhandlet i litra c), begrundes i tilfælde, hvor hændelsen stadig er i gang.**

5. De kompetente nationale myndigheder eller CSIRT'en skal [...] **uden unødig forsinkelse** efter modtagelsen af den i artikel 4, litra a), omhandlede indledende underretning give den underrettende enhed et svar, herunder indledende tilbagemeldinger om hændelsen og, efter anmodning fra enheden, vejledning om gennemførelsen af mulige afbødende foranstaltninger. Hvis CSIRT'en ikke har modtaget den i stk. 1 omhandlede underretning, gives vejledningen af den kompetente myndighed i samarbejde med CSIRT'en. CSIRT'en yder supplerende teknisk bistand, hvis den berørte enhed anmoder herom. Hvis hændelsen mistænkes for at være af strafferetlig karakter, giver de kompetente nationale myndigheder eller CSIRT'en også vejledning om underretning af retshåndhævende myndigheder om hændelsen.

6. Hvis det er relevant, og navnlig hvor den i stk. 1 omhandlede hændelse berører to eller flere medlemsstater, informerer den kompetente myndighed eller CSIRT'en eller **det centrale kontaktpunkt** de øvrige berørte medlemsstater og ENISA om hændelsen. **Sådanne oplysninger skal mindst omfatte de elementer, der er omhandlet i stk. 4 i denne artikel.** De kompetente myndigheder, CSIRT'erne og de centrale kontaktpunkter sikrer i den forbindelse i overensstemmelse med EU-retten eller national lovgivning, der er i overensstemmelse med EU-retten, den digitale tjenesteudbyders sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger.

7. Hvis offentlighedens kendskab er nødvendig for at forebygge en hændelse eller for at håndtere en igangværende hændelse, eller hvis offentliggørelse af hændelsen på anden vis er i offentlighedens interesse, kan den kompetente myndighed eller CSIRT'en og, hvor det er relevant, myndighederne eller CSIRT'erne i andre berørte medlemsstater efter høring af den berørte enhed informere offentligheden om hændelsen eller kræve, at enheden gør det.

8. På den kompetente myndigheds eller CSIRT'ens anmodning videresender det centrale kontaktpunkt de i stk. [...] 1 [...] omhandlede underretninger til centrale kontaktpunkter i andre berørte medlemsstater.

9. Det centrale kontaktpunkt forelægger [...] **hver sjette måned** en sammenfattende rapport for ENISA, herunder anonymiserede og aggregerede data om hændelser, væsentlige cybertrusler og nærvedhændelser, der er underrettet om i overensstemmelse med stk. [...] 1 [...] og i overensstemmelse med artikel 27. For at bidrage til tilvejebringelsen af sammenlignelige oplysninger kan ENISA udstede teknisk vejledning om parametrene for oplysningerne i den sammenfattende rapport. **ENISA underretter hver sjette måned samarbejdsgruppen og CSIRT-netværket om sine resultater vedrørende de modtagne underretninger.**

10. De kompetente myndigheder giver de kompetente myndigheder, der er udpeget i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed], oplysninger om hændelser og cybertrusler, som er meddelt i overensstemmelse med stk. 1 og 2 af væsentlige enheder, der er identificeret som kritiske enheder **[**eller som enheder, der svarer til kritiske enheder,**]** i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed].

11. Kommissionen kan vedtage gennemførelsesretsakter, der yderligere præciserer typen af oplysninger, formatet og proceduren for en meddelelse indgivet i henhold til stk. 1 og 2. Kommissionen kan også vedtage gennemførelsesretsakter for yderligere at præcisere de tilfælde, hvor en hændelse anses for at være væsentlig, jf. stk. 3. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 37, stk. 2.

Artikel 21

Brug af europæiske cybersikkerhedscertificeringsordninger

1. For at påvise overensstemmelse med visse krav i artikel 18 **kan medlemsstaterne kræve, at enheder anvender bestemte IKT-produkter,** [...] **-tjenester og** [...] **-processer**, **der er certificeret** i henhold til specifikke europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i henhold til artikel 49 i forordning (EU) 2019/881. De **IKT-**produkter, tjenester og processer, der certificeres, kan være udviklet af en væsentlig eller vigtig enhed eller indkøbes fra tredjeparter.

2. Kommissionen kan [...] vedtage [...] **gennemførelses**retsakter, som præciserer, hvilke kategorier af væsentlige **eller vigtige** enheder der skal **anvende visse certificerede IKT-produkter, -tjenester og -processer eller** indhente en attest [...] og i henhold til hvilke [...] europæiske cybersikkerhedscertificeringsordninger**, der er vedtaget i henhold til artikel 49 i forordning (EU) 2019/881.**[...] **Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 37, stk. 2. Ved udarbejdelse af sådanne gennemførelsesretsakter skal Kommissionen i overensstemmelse med artikel 56 i forordning (EU) 2019/881:**

   i) **tage hensyn til foranstaltningernes indvirkning på producenter og udbydere af sådanne IKT-produkter, -tjenester og -processer og på brugerne i form af omkostninger ved disse foranstaltninger og de samfundsmæssige eller økonomiske fordele som følge af det forventede øgede sikkerhedsniveau for de pågældende IKT-produkter, -tjenester og -processer samt deres alternative tilgængelighed på markedet**

   ii) **gennemføre en åben, gennemsigtig og inklusiv høringsproces med alle relevante interessenter og medlemsstater**

(iii) tage hensyn til eventuelle gennemførelsesfrister og overgangsforanstaltninger eller -perioder under hensyntagen til navnlig foranstaltningernes mulige indvirkning på producenter eller udbydere af IKT-produkter, -tjenester og -processer og på brugerne heraf, navnlig SMV'er

(iv) tage hensyn til eksistensen og gennemførelsen af relevant ret i medlemsstaterne.

3. Kommissionen kan anmode ENISA om at udarbejde et forslag til ordning **eller om en revision af en eksisterende europæisk certificeringsordning vedrørende cybersikkerhed** i henhold til artikel 48, stk. 2, i forordning (EU) 2019/881 i tilfælde, hvor der ikke findes en passende europæisk cybersikkerhedscertificeringsordning, jf. stk. 2.

Artikel 22

Standardisering

1. For at sikre en samordnet gennemførelse af artikel 18, stk. 1 og 2, tilskynder medlemsstaterne til at benytte europæiske eller internationalt anerkendte standarder og specifikationer, der er relevante for sikkerheden i net- og informationssystemer, uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi.

2. ENISA udarbejder i samarbejde med medlemsstaterne vejledning og retningslinjer om de tekniske områder, der skal overvejes i forbindelse med stk. 1, samt om allerede eksisterende standarder, herunder medlemsstaternes nationale standarder, hvilket vil give mulighed for at dække disse områder.

Artikel 23

Database over domænenavne og registreringsoplysninger

1. Med henblik på at bidrage til DNS' sikkerhed, stabilitet og modstandsdygtighed sikrer medlemsstaterne, at topdomæne**navne**administratorer og enheder, der udbyder domænenavnsregistreringstjenester til topdomæner, med rettidig omhu indsamler og vedligeholder nøjagtige [...] og fuldstændige oplysninger om domænenavnsregistrering i en særlig databasefacilitet **i overensstemmelse med** [...] Unionens databeskyttelseslovgivning for så vidt angår personoplysninger.

2. Medlemsstaterne sikrer, at de i stk. 1 omhandlede databaser over domænenavnsregistreringsdata indeholder relevante oplysninger med henblik på at identificere og kontakte indehaverne af domænenavne og de kontaktpunkter, der forvalter domænenavne under topdomæner**, der som minimum omfatter følgende:**

   a) domænenavn

   b) registreringsdato

   c) oplysninger om registranten, herunder:

      i) for fysiske personer – fornavn, efternavn og e-mailadresse

      ii) for juridiske personer – navn og e-mailadresse.

3. Medlemsstaterne sikrer, at topdomæne**navne**administratorerne og de enheder, der udbyder domænenavnsregistreringstjenester til topdomæner, har indført politikker og procedurer, der sikrer, at databaserne indeholder nøjagtige og fuldstændige oplysninger. Medlemsstaterne sikrer, at sådanne politikker og procedurer gøres offentligt tilgængelige.

4. Medlemsstaterne sikrer, at topdomæne**navne**administratorerne og de enheder, der udbyder domænenavnsregistreringstjenester til topdomæner, uden unødig forsinkelse efter registreringen af et domænenavn offentliggør domæneregistreringsdata, som ikke er personoplysninger.

5. Medlemsstaterne sikrer, at topdomæne**navne**administratorerneog de enheder, der udbyder domænenavnsregistreringstjenester til topdomæner, giver adgang til specifikke oplysninger om domænenavnsregistrering efter lovlige og behørigt begrundede anmodninger fra legitime adgangssøgende i overensstemmelse med EU's databeskyttelseslovgivning. Medlemsstaterne sikrer, at topdomæne**navne**administratorerne og de enheder, der udbyder domænenavnsregistreringstjenester til topdomæner, besvarer alle anmodninger om adgang uden unødig forsinkelse **og under alle omstændigheder inden for 72 timer**. Medlemsstaterne sikrer, at politikker og procedurer for offentliggørelse af sådanne data gøres offentligt tilgængelige.

Afsnit II

Jurisdiktion og registrering

Artikel 24

Jurisdiktion og territorialitet

1a. Enheder i henhold til dette direktiv anses for at høre under jurisdiktionen i den medlemsstat, hvor de udbyder deres tjenester. De enheder, der er omhandlet i punkt 1-7 og punkt 10 i bilag I, tillidstjenesteudbydere og udbydere af internetudvekslingspunkter, der er omhandlet i punkt 8 i bilag I, og punkt 1-5 i bilag II, anses for at høre under medlemsstatens jurisdiktion på det område, hvor de er etableret.

1. DNS-tjenesteudbydere, topdomænenavneadministratorer, [...] **og enheder, der udbyder domænenavnsregistreringstjenester til topdomæner**, udbydere af cloudcomputingtjenester, udbydere af datacentertjenester, [...] udbydere af indholdsudsendelsesnetværk, **udbydere af administrerede tjenester og udbydere af administrerede sikkerhedstjenester**, jf. bilag I, punkt 8 **og 8a**, samt digitale udbydere som omhandlet i bilag II, punkt 6, anses for at høre under jurisdiktionen i den medlemsstat, hvor de har deres hovedforretningssted i Unionen.

2. Med henblik på dette direktiv anses enhederne, der er omhandlet i stk. 1, for at have deres hovedvirksomhed i Unionen i den medlemsstat, hvor beslutningerne vedrørende foranstaltningerne til styring af cybersikkerhedsrisici **overvejende** træffes. Hvis **det sted, hvor sådanne beslutninger overvejende træffes, ikke kan fastslås, eller** sådanne beslutninger ikke træffes i en virksomhed i Unionen, anses hovedvirksomheden for at ligge i den medlemsstat, hvor enhederne har virksomheden med det største antal ansatte i Unionen. **Når tjenesterne udbydes af en gruppe af virksomheder, anses hovedvirksomheden for at være gruppen af virksomheders hovedvirksomhed.**

3. Hvis en enhed som omhandlet i stk. 1 ikke er etableret i Unionen, men udbyder tjenester inden for Unionen, udpeger den en repræsentant i Unionen. Repræsentanten skal være etableret i en af de medlemsstater, hvor tjenesterne tilbydes. En sådan enhed anses for at høre under den medlemsstats jurisdiktion, hvor repræsentanten er etableret. Hvis der ikke findes en udpeget repræsentant i Unionen i henhold til denne artikel, kan enhver medlemsstat, hvor enheden leverer tjenester, anlægge sag mod enheden for manglende overholdelse af forpligtelserne i henhold til dette direktiv.

4. En i stk. 1 omhandlet enheds udpegelse af en repræsentant berører ikke eventuelle retlige skridt mod selve udbyderen af digitale tjenester.

4a. Medlemsstater, der har modtaget en anmodning om gensidig bistand vedrørende de enheder, der er omhandlet i stk. 1, kan inden for rammerne af anmodningen træffe passende tilsyns- og håndhævelsesforanstaltninger over for den pågældende enhed, der udbyder tjenester, eller som har net- og informationssystemer på deres område.

Artikel 25

Register over visse enheder inden for digital infrastruktur og digitale udbydere

1. [...] **Medlemsstaterne sikrer, at de** [...] enheder, **der er omhandlet i artikel 24, stk. 1, og som har deres hovedvirksomhed på deres område, eller hvis de ikke er etableret i Unionen, som har deres udpegede repræsentant i Unionen etableret på deres område, skal** [...] fremsende følgende oplysninger **til de kompetente myndigheder** [...] senest [12 måneder efter direktivets ikrafttræden]:

a) enhedens navn

aa) typen af enhed ifølge dette direktivs bilag I og II

b) adressen på dens hovedvirksomhed og andre retlige enheder i Unionen eller, hvis den ikke er etableret i Unionen, på den repræsentant, der er udpeget i henhold til artikel 24, stk. 3

c) ajourførte kontaktoplysninger, herunder e-mailadresser og telefonnumre på enhederne **og deres repræsentanter**

d) de medlemsstater, hvor enheden udbyder tjenesten.

Hvis det er relevant, fremsendes disse oplysninger gennem den nationale mekanisme[...] til selvunderretning, der er omhandlet i artikel 2a.

2. **Medlemsstaterne skal sikre, at**de i stk. 1 omhandlede enheder **også** straks og under alle omstændigheder senest tre måneder efter den dato, hvor ændringen trådte i kraft, **underretter** om enhver ændring af de oplysninger, de har indsendt i henhold til stk. 1.

3. [...] **Medlemsstaternes centrale kontaktpunkter** fremsender **de i stk. 1 og stk. 2 omhandlede oplysninger** [...] til [...] **ENISA**. [...]

3a. På grundlag af de oplysninger, der modtages i overensstemmelse med denne artikels stk. 3, opretter og vedligeholder ENISA et register over de enheder, der er omhandlet i stk. 1. Efter anmodning fra medlemsstaterne giver ENISA de relevante kompetente myndigheder adgang til registret, samtidig med at det sikrer de nødvendige garantier for at beskytte fortroligheden af oplysninger, hvor det er relevant.

4. [...]

KAPITEL V

Udveksling af oplysninger

Artikel 26

Ordninger for udveksling af cybersikkerhedsoplysninger

1. [...] Medlemsstaterne sikrer, at væsentlige og vigtige enheder **frivilligt** kan udveksle relevante cybersikkerhedsoplysninger indbyrdes, herunder oplysninger om cybertrusler, **nærvedhændelser**, sårbarheder, kompromitteringsindikatorer, taktikker, teknikker og procedurer, cybersikkerhedsadvarsler og konfigurationsværktøjer, hvis denne informationsudveksling:

   a) har til formål at forebygge, opdage, reagere på eller afbøde hændelser

b) øger cybersikkerhedsniveauet, navnlig ved at øge bevidstheden om cybertrusler, begrænse eller hindre sådanne truslers evne til at sprede sig, støtte en række forsvarskapaciteter, afhjælpe og offentliggøre sårbarheder, teknikker til sporing af trusler, afbødningsstrategier eller indsats- og genopretningsfaser.

2. Medlemsstaterne sikrer, at udvekslingen af oplysninger finder sted inden for [...] fællesskaber af væsentlige og vigtige enheder. En sådan udveksling gennemføres ved hjælp af ordninger for udveksling af oplysninger for så vidt angår den potentielt følsomme karakter af de udvekslede oplysninger [...].

3. Medlemsstaterne [...] **kan** fastsætte regler, der præciserer proceduren, de operationelle elementer (herunder brugen af særlige IKT-platforme), indholdet af og betingelserne for de i stk. 2 omhandlede informationsudvekslingsordninger. Sådanne regler [...] **kan** også indeholde nærmere bestemmelser om inddragelse af offentlige myndigheder i sådanne ordninger samt operationelle elementer, herunder brug af særlige IT-platforme. Medlemsstaterne yder støtte til anvendelsen af sådanne ordninger i overensstemmelse med deres politikker, jf. artikel 5, stk. 2, litra g).

4. Væsentlige og vigtige enheder underretter de kompetente myndigheder om deres deltagelse i de i stk. 2 omhandlede informationsudvekslingsordninger, når de indtræder i sådanne ordninger, eller, hvis det er relevant, om deres udtræden af sådanne ordninger, når denne udtræden træder i kraft.

5. [...] ENISA støtter oprettelsen af ordninger for udveksling af cybersikkerhedsoplysninger som omhandlet i stk. 2 ved at levere bedste praksis og vejledning.

Artikel 27

Frivillig underretning om relevante oplysninger

1. Med forbehold af artikel 20 sikrer medlemsstaterne, at væsentlige og vigtige enheder frivilligt kan underrette de kompetente myndigheder eller CSIRT'erne om relevante hændelser, cybertrusler eller nærvedhændelser.

2. Medlemsstaterne sikrer, at enheder, der falder uden for dette direktivs anvendelsesområde, med forbehold af artikel 3 kan foretage underretninger på frivillig basis om væsentlige hændelser, cybertrusler eller nærvedhændelser. Når medlemsstaterne behandler underretninger, handler de efter proceduren i artikel 20. Medlemsstaterne kan prioritere behandling af obligatoriske underretninger frem for frivillige underretninger. **Uden at det berører efterforskning, afsløring og retsforfølgning af strafbare handlinger,** må [...] frivillige underretninger ikke medføre, at den underrettende enhed pålægges nogen yderligere forpligtelser, som den ikke ville være omfattet af, hvis den ikke havde foretaget denne underretning.

3. Frivillige underretninger behandles udelukkende, når en sådan behandling ikke udgør en uforholdsmæssig stor eller unødvendig byrde for den berørte medlemsstat.

KAPITEL VI

Tilsyn og håndhævelse

Artikel 28

Generelle aspekter vedrørende tilsyn og håndhævelse

1. Medlemsstaterne sikrer, at de kompetente myndigheder effektivt overvåger og træffer de nødvendige foranstaltninger for at sikre, at dette direktiv overholdes [...], navnlig forpligtelserne i artikel 18**,** [...] 20 **og 23**. **Medlemsstaterne kan give de kompetente myndigheder mulighed for at prioritere tilsyn, som er baseret på en risikobaseret tilgang.**

2. De kompetente myndigheder indgår i et tæt samarbejde med databeskyttelsesmyndigheder**, kompetente myndigheder udpeget i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed], tilsynsorganer udpeget i henhold til forordning (EU) nr. 910/2014 og andre kompetente myndigheder udpeget i medfør af sektorspecifikke EU-retsakter**, når de håndterer cybersikkerhedshændelser. [...]

3. Med forbehold af nationale lovgivningsmæssige og institutionelle rammer sikrer medlemsstaterne, at de kompetente myndigheder i forbindelse med tilsynet med offentlige forvaltningsenheders overholdelse af dette direktiv og håndhævelsen af potentielle sanktioner for manglende overholdelse har de nødvendige beføjelser til at udføre sådanne opgaver med operationel uafhængighed i forhold til de enheder, der føres tilsyn med. Medlemsstaterne kan beslutte at indføre passende, forholdsmæssige og effektive tilsyns- og håndhævelsesforanstaltninger over for disse enheder i overensstemmelse med de nationale rammer og det nationale retssystem.

Artikel 29

Tilsyn og håndhævelse for væsentlige enheder

1. Medlemsstaterne sikrer, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder for så vidt angår de forpligtelser, som er fastsat i dette direktiv, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i den enkelte sag.

2. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udfører deres tilsynsopgaver i forbindelse med væsentlige enheder, **følger en risikobaseret tilgang og** har beføjelse til **som minimum** at pålægge disse enheder:

   a) kontrol på stedet og tilsyn uden for stedet, herunder stikprøvekontrol

   b) regelmæssige **sikkerheds**revisioner

   c) målrettede sikkerhedsrevisioner baseret på risikovurderinger eller risikorelaterede tilgængelige oplysninger

   d) sikkerhedsscanninger baseret på objektive, ikkediskriminerende, retfærdige og gennemsigtige risikovurderingskriterier**, hvis det er nødvendigt af tekniske årsager, i samarbejde med den berørte enhed**

   e) anmodninger om oplysninger, der er nødvendige for at vurdere enhedens cybersikkerhedsforanstaltninger, herunder dokumenterede cybersikkerhedspolitikker[...]

   f) anmodninger om adgang til data, dokumenter eller oplysninger, der er nødvendige for udførelsen af deres tilsynsopgaver

   g) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsrevisioner udført af en kvalificeret revisor og den respektive underliggende dokumentation.

2a. De kompetente myndigheder kan, når de udfører deres tilsynsopgaver som omhandlet i denne artikels stk. 2, indføre tilsynsmetoder, der gør det muligt at prioritere sådanne opgaver efter en risikobaseret tilgang.

3. Ved udøvelsen af deres beføjelser i henhold til stk. 2, litra e)-g), angiver de kompetente myndigheder formålet med anmodningen og præciserer, hvilke oplysninger der anmodes om.

4. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udøver deres håndhævelsesbeføjelser over for væsentlige enheder, **som minimum** har beføjelse til at:

   a) udstede advarsler om enhedernes manglende overholdelse af forpligtelserne i dette direktiv

   b) udstede bindende instrukser eller pålægge disse enheder at afhjælpe de konstaterede mangler eller overtrædelserne af de forpligtelser, der er fastsat i dette direktiv

   c) pålægge disse enheder at ophøre med at udvise adfærd, der ikke opfylder de forpligtelser, som er fastsat i dette direktiv, og afstå fra at gentage denne adfærd

   d) pålægge disse enheder at bringe deres risikostyringsforanstaltninger og/eller rapporteringsforpligtelser i overensstemmelse med forpligtelserne i artikel 18 og 20 på en nærmere bestemt måde og inden for en nærmere angivet frist

   e) pålægge disse enheder at underrette den eller de fysiske eller juridiske personer, som de udbyder tjenester eller aktiviteter til, og som potentielt er berørt af en væsentlig cybertrussel, om **denne trussels karakter og** eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som disse fysiske eller juridiske personer kan træffe som reaktion på denne trussel

   f) pålægge disse enheder at gennemføre de anbefalinger, der er fremsat som følge af en sikkerhedsrevision, inden for en rimelig frist

   g) [...]

h) pålægge disse enheder at offentliggøre aspekter af manglende overholdelse af forpligtelserne i dette direktiv på en nærmere angivet måde**, når en sådan offentliggørelse ikke medfører skadelig eksponering af den pågældende enhed**

i) [...]

j) pålægge eller anmode de relevante organer eller domstole om i henhold til national lovgivning at pålægge en administrativ bøde i henhold til artikel 31 ud over eller i stedet for de foranstaltninger, der er omhandlet i dette stykkes litra a)-i), afhængigt af omstændighederne i den enkelte sag.

5. Hvis håndhævelsesforanstaltninger vedtaget i henhold til stk. 4, litra a)-d) og f), viser sig at være virkningsløse, sikrer medlemsstaterne, at de kompetente myndigheder har beføjelse til at fastsætte en frist, inden for hvilken den væsentlige enhed anmodes om at træffe de nødvendige foranstaltninger for at afhjælpe manglerne eller opfylde disse myndigheders krav. Hvis den ønskede foranstaltning ikke træffes inden for den fastsatte frist, sikrer medlemsstaterne, at de kompetente myndigheder har beføjelse til at:

a) suspendere eller anmode et certificerings- eller godkendelsesorgan **eller domstole i overensstemmelse med national lovgivning** om at suspendere en certificering eller godkendelse vedrørende dele af eller alle de tjenester eller aktiviteter, der udbydes af en væsentlig enhed

b) pålægge eller anmode de relevante organer eller domstole om i henhold til national lovgivning midlertidigt at forbyde enhver person med ledelsesansvar på administrerende eller juridisk niveau i den pågældende væsentlige enhed og enhver anden fysisk person, der anses for at være ansvarlig for overtrædelsen, at udøve ledelsesfunktioner i den pågældende enhed.

Disse sanktioner anvendes kun, indtil enheden træffer de nødvendige foranstaltninger for at afhjælpe manglerne eller opfylde kravene fra den kompetente myndighed, for hvilken sådanne sanktioner blev anvendt.

De i dette stykke omhandlede sanktioner finder ikke anvendelse på offentlige forvaltningsenheder, der er omfattet dette direktiv.

6. Medlemsstaterne sikrer, at enhver fysisk person, der er ansvarlig for eller optræder som repræsentant for en væsentlig enhed på grundlag af beføjelsen til at repræsentere den, beføjelsen til at træffe afgørelser på dennes vegne eller beføjelsen til at udøve kontrol over den, har beføjelse til at sikre, at enheden overholder forpligtelserne i dette direktiv. Medlemsstaterne sikrer, at disse fysiske personer kan drages til ansvar for tilsidesættelse af deres forpligtelser til at sikre overholdelse af forpligtelserne i dette direktiv. **Med hensyn til offentlige forvaltningsenheder berører denne bestemmelse ikke medlemsstaternes lovgivning for så vidt angår offentlige ansattes og valgte og udnævnte tjenestemænds ansvar.**

7. Når de kompetente myndigheder træffer håndhævelsesforanstaltninger eller anvender sanktioner i henhold til stk. 4 og 5, skal de overholde retten til forsvar og tage hensyn til omstændighederne i den enkelte sag og som minimum tage behørigt hensyn til:

   a) overtrædelsens grovhed og betydningen af de tilsidesatte bestemmelser. Blandt de overtrædelser, der bør betragtes som alvorlige: gentagne overtrædelser, manglende underretning om eller afhjælpning af hændelser med en betydelig forstyrrende virkning, manglende afhjælpning af mangler som følge af bindende instrukser fra de kompetente myndigheder, der lægger hindringer i vejen for revisioner eller overvågningsaktiviteter, som den kompetente myndighed har beordret efter konstatering af en overtrædelse, afgivelse af urigtige eller klart unøjagtige oplysninger i forbindelse med risikostyringskravene eller rapporteringsforpligtelserne i artikel 18 og 20

b) overtrædelsens varighed, herunder elementet af gentagne overtrædelser

c) de faktiske skader eller lidte tab eller potentielle skader eller tab, der kunne være blevet udløst, for så vidt de kan fastslås. Ved evalueringen af dette aspekt skal der bl.a. tages hensyn til faktiske eller potentielle finansielle eller økonomiske tab, virkninger for andre tjenester, antal brugere, der er berørt eller potentielt berørt

d) hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt

e) foranstaltninger, som enheden har truffet for at forebygge eller afbøde skaden og/eller tabet

f) overholdelse af godkendte adfærdskodekser eller godkendte certificeringsmekanismer

g) graden af samarbejde mellem den eller de fysiske eller juridiske person(er), der gøres ansvarlig(e), og de kompetente myndigheder.

8. De kompetente myndigheder skal give en detaljeret begrundelse for deres håndhævelsesafgørelser. Inden de kompetente myndigheder træffer sådanne afgørelser, underretter de de berørte enheder om deres foreløbige resultater og giver disse enheder en rimelig frist til at fremsætte bemærkninger**, medmindre der er tale om en overhængende fare**.

9. Medlemsstaterne sikrer, at deres kompetente myndigheder **i henhold til dette direktiv** underretter de relevante kompetente myndigheder **i den samme** [...] medlemsstat [...], der er udpeget i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed], når de udøver deres tilsyns- og håndhævelsesbeføjelser med henblik på at sikre, at en væsentlig enhed, der er identificeret som kritisk **[**eller som en enhed svarende til en kritisk enhed**]**, i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed] overholder forpligtelserne i henhold til dette direktiv. **Hvis det er relevant, kan** de kompetente myndigheder i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed][...] **anmode** de kompetente myndigheder **i henhold til dette direktiv** [...] **om at** udøve deres tilsyns- og håndhævelses**beføjelser over for** en væsentlig enhed, jf. dette direktivs anvendelsesområde, der også er identificeret som kritisk **[**eller tilsvarende**] i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed].**

10. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv underretter tilsynsforummet, jf. artikel 29, stk. 1, i forordning (EU) XXXX/XXXX [DORA], når de udøver deres tilsyns- og håndhævelsesbeføjelser, med det formål at sikre, at en væsentlig enhed, der er udpeget som tredjepartstjenesteudbyder af kritisk IKT, jf. artikel 28 i forordning (EU) XXXX/XXXX [DORA], overholder forpligtelserne i dette direktiv.

10a. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv underretter de relevante kompetente myndigheder udpeget i henhold til forordning (EU) nr. 910/2014, når de udøver deres tilsyns- og håndhævelsesbeføjelser med det formål at sikre, at en enhed, der er udpeget som tillidstjenesteudbyder, jf. forordning (EU) nr. 910/2014, overholder forpligtelserne i dette direktiv.

Artikel 30

Tilsyn og håndhævelse for vigtige enheder

1. Hvis der forelægges dokumentation for eller er tegn på **eller oplysninger** om, at en vigtig enhed **angiveligt** ikke overholder forpligtelserne i dette direktiv, særlig artikel 18 og 20, sikrer medlemsstaterne, at de kompetente myndigheder træffer foranstaltninger, hvor det er nødvendigt, gennem efterfølgende tilsynsforanstaltninger.

2. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udfører deres tilsynsopgaver i forbindelse med vigtige enheder, **følger en risikobaseret tilgang og** har beføjelse til **som minimum** at pålægge disse enheder:

   a) kontrol på stedet og efterfølgende tilsyn uden for stedet

   b) målrettede sikkerhedsrevisioner baseret på risikovurderinger eller risikorelaterede tilgængelige oplysninger

   c) sikkerhedsscanninger baseret på objektive, **ikkediskriminerende,** retfærdige og gennemsigtige risikovurderingskriterier**, hvis det er nødvendigt af tekniske årsager, i samarbejde med den berørte enhed**

   d) anmodninger om oplysninger, der er nødvendige for efterfølgende at vurdere cybersikkerhedsforanstaltningerne[...]

   e) anmodninger om adgang til data, dokumenter og/eller oplysninger, der er nødvendige for udførelsen af tilsynsopgaverne

   ea) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsrevisioner udført af en kvalificeret revisor og den respektive underliggende dokumentation.

2a. De kompetente myndigheder kan, når de udfører deres tilsynsopgaver som omhandlet i denne artikels stk. 2, indføre tilsynsmetoder, der gør det muligt at prioritere sådanne opgaver efter en risikobaseret tilgang.

3. Ved udøvelsen af deres beføjelser i henhold til stk. 2, litra d)**-ea)**, angiver de kompetente myndigheder formålet med anmodningen og præciserer, hvilke oplysninger der anmodes om.

4. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udøver deres håndhævelsesbeføjelser over for vigtige enheder, har beføjelse til **som minimum** at:

   a) udstede advarsler om enhedernes manglende overholdelse af forpligtelserne i dette direktiv

   b) udstede bindende instrukser eller pålægge disse enheder at afhjælpe de konstaterede mangler eller overtrædelserne af de forpligtelser, der er fastsat i dette direktiv

   c) pålægge disse enheder at ophøre med at udvise en adfærd, der ikke opfylder de forpligtelser, som er fastsat i dette direktiv, og afstå fra at gentage denne adfærd

   d) pålægge disse enheder at bringe deres risikostyringsforanstaltninger eller underretningsforpligtelser i overensstemmelse med de forpligtelser, der er fastsat i artikel 18 og 20, på en nærmere angivet måde og inden for en nærmere angivet frist

   e) pålægge disse enheder at underrette den eller de fysiske eller juridiske personer, som de udbyder tjenester eller aktiviteter til, og som potentielt er berørt af en væsentlig cybertrussel, om **denne trussels karakter og** eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som disse fysiske eller juridiske personer kan træffe som reaktion på denne trussel

   f) pålægge disse enheder at gennemføre de anbefalinger, der er fremsat som følge af en sikkerhedsrevision, inden for en rimelig frist

g) pålægge disse enheder at offentliggøre aspekter af manglende overholdelse af deres forpligtelser i henhold til dette direktiv på en nærmere angivet måde**, når en sådan offentliggørelse ikke medfører skadelig eksponering af den pågældende enhed**

h) [...]

i) pålægge eller anmode de relevante organer eller domstole om i henhold til national lovgivning at pålægge en administrativ bøde i henhold til artikel 31 ud over eller i stedet for de foranstaltninger, der er omhandlet i dette stykkes litra a)-h), afhængigt af omstændighederne i den enkelte sag.

5. Artikel 29, stk. 6-8, finder også anvendelse på tilsyns- og håndhævelsesforanstaltningerne i denne artikel for [...] vigtige enheder [...].

Artikel 31

Generelle betingelser for pålæggelse af administrative bøder

1. Medlemsstaterne sikrer, at administrative bøder, der pålægges væsentlige og vigtige enheder i henhold til denne artikel for overtrædelse af de forpligtelser, som er fastsat i dette direktiv, i hvert enkelt tilfælde er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning.

2. Administrative bøder pålægges afhængigt af omstændighederne i hver enkelt sag i tillæg til eller i stedet for foranstaltninger som omhandlet i artikel 29, stk. 4, litra a)-i), artikel 29, stk. 5, og artikel 30, stk. 4, litra a)-h).

3. Når det skal besluttes, om der skal pålægges en administrativ bøde, og der træffes afgørelse om dens størrelse i hvert enkelt tilfælde, tages der som minimum behørigt hensyn til de i artikel 29, stk. 7, omhandlede elementer.

4. Medlemsstaterne sikrer, at overtrædelser begået af **væsentlige enheder** af forpligtelserne i artikel 18 eller artikel 20 i overensstemmelse med nærværende artikels stk. 2 og 3 straffes med administrative bøder på maksimalt mindst **4**[...] 000 000 EUR eller, **hvis det drejer sig om en juridisk person**, [...] 2 % af den samlede globale årsomsætning i den virksomhed, som den væsentlige [...] enhed tilhører, i det foregående regnskabsår, alt efter hvad der er højest.

4a. Medlemsstaterne sikrer, at overtrædelser begået af vigtige enheder af forpligtelserne i artikel 18 eller artikel 20 i overensstemmelse med nærværende artikels stk. 2 og 3 straffes med administrative bøder på maksimalt mindst 2 000 000 EUR eller, hvis det drejer sig om en juridisk person, 1 % af den samlede globale årsomsætning i den virksomhed, som den vigtige enhed tilhører, i det foregående regnskabsår, alt efter hvad der er højest.

5. Medlemsstaterne kan fastsætte beføjelser til at pålægge tvangsbøder for at tvinge en væsentlig eller vigtig enhed til at bringe en overtrædelse til ophør i overensstemmelse med en forudgående afgørelse truffet af den kompetente myndighed.

6. Uden at det berører tilsynsmyndighedernes korrigerende beføjelser i henhold til artikel 29 og 30, kan hver medlemsstat fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige forvaltningsorganer, jf. artikel 4, nr. 23, i henhold til bestemmelserne i nærværende direktiv.

6a. Hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, sikrer medlemsstaterne, at denne artikel anvendes på en sådan måde, at den kompetente myndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af de kompetente myndigheder. Bøder skal under alle omstændigheder være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. De pågældende medlemsstater giver Kommissionen meddelelse om bestemmelserne i de love, som de vedtager i henhold til dette stykke, senest den [...] og underretter den straks om alle senere ændringslove eller ændringer, der berører dem.

Artikel 32

Overtrædelser, der medfører brud på persondatasikkerheden

1. Hvis de kompetente myndigheder **som led i tilsynet eller håndhævelsen** får [...] **kendskab til**, at en væsentlig eller vigtig enheds overtrædelse af de forpligtelser, der er fastsat i **dette direktivs** artikel 18 og 20, **kan** medføre [...] et brud på persondatasikkerheden som omhandlet i artikel 4, stk. 12, i forordning (EU) 2016/679, som skal anmeldes i henhold til nævnte forordnings artikel 33, underretter de **uden unødig forsinkelse** de tilsynsmyndigheder, der er kompetente i henhold til nævnte forordnings artikel 55 og 56 [...].

2. Hvis de tilsynsmyndigheder, der er kompetente i henhold til artikel 55 og 56 i forordning (EU) 2016/679, beslutter at udøve deres beføjelser i henhold til artikel 58, **stk. 2,** litra i), i nævnte forordning og pålægger en administrativ bøde, pålægger de **i dette direktivs artikel 8 omhandlede** kompetente myndigheder ikke en administrativ bøde for [...] **en** overtrædelse **for den samme handling** i henhold til [...] dette direktivs artikel 31. De kompetente myndigheder kan dog anvende de håndhævelsesforanstaltninger eller udøve de sanktionsbeføjelser, der er omhandlet i dette direktivs artikel 29, stk. 4, litra a)-i), artikel 29, stk. 5, og artikel 30, stk. 4, litra a)-h).

3. Hvis den tilsynsmyndighed, der er kompetent i henhold til forordning (EU) 2016/679, er etableret i en anden medlemsstat end den kompetente myndighed, kan den kompetente myndighed underrette tilsynsmyndigheden, der er etableret i samme medlemsstat.

Artikel 33

Sanktioner

1. Medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale regler, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger til at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

2. Medlemsstaterne giver senest [to] år efter dette direktivs ikrafttræden Kommissionen meddelelse om disse regler og foranstaltninger og underretter den uden unødig forsinkelse om alle senere ændringer, der berører dem.

Artikel 34

Gensidig bistand

1. Hvis en væsentlig eller vigtig enhed udbyder tjenester i mere end én medlemsstat eller [...] **udbyder tjenester** i **en eller flere** medlemsstat**er**, men dens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder de kompetente myndighed[...]**er** i de **pågældende** medlemsstat**er** [...] og bistår hinanden efter behov. Dette samarbejde indebærer som minimum, at:

a) de kompetente myndigheder, der anvender tilsyns- eller håndhævelsesforanstaltninger i en medlemsstat, via det fælles kontaktpunkt underretter og hører de kompetente myndigheder i de øvrige berørte medlemsstater om de tilsyns- og håndhævelsesforanstaltninger, der er truffet [...]

b) en kompetent myndighed kan anmode en anden kompetent myndighed om at træffe tilsyns- eller håndhævelsesforanstaltninger [...]

c) en kompetent myndighed efter modtagelse af en begrundet anmodning fra en anden kompetent myndighed yder bistand**, der står i et rimeligt forhold til de ressourcer, den har til rådighed,** til den anden kompetente myndighed, således at tilsyns- eller håndhævelsesforanstaltningerne [...] kan gennemføres på en effektiv, virkningsfuld og konsekvent måde. En sådan gensidig bistand kan omfatte anmodninger om oplysninger og tilsynsforanstaltninger, herunder anmodninger om at foretage inspektioner på stedet eller tilsyn uden for stedet eller målrettede sikkerhedskontroller. En kompetent myndighed, som en anmodning om bistand er rettet til, kan ikke afvise anmodningen, medmindre det efter en udveksling med de øvrige berørte myndigheder [...] fastslås, [...] at myndigheden ikke er kompetent til at yde den ønskede bistand, **ikke har de fornødne ressourcer,** eller at den bistand, der anmodes om, ikke står i et rimeligt forhold til den kompetente myndigheds udførte tilsynsopgaver, [...] **eller hvis anmodningen vedrører oplysninger eller indebærer aktiviteter, der er i strid med den pågældende medlemsstats nationale sikkerhed eller offentlige sikkerhed eller forsvar**.

2. Når det er hensigtsmæssigt og efter fælles overenskomst, kan kompetente myndigheder fra forskellige medlemsstater gennemføre fælles tilsynsforanstaltninger [...].

KAPITEL VII

Overgangsbestemmelser og afsluttende bestemmelser

Artikel 35

Evaluering

Kommissionen tager regelmæssigt dette direktivs funktion op til evaluering og forelægger en rapport for Europa-Parlamentet og Rådet. Rapporten skal navnlig vurdere relevansen af de i bilag I og II omhandlede sektorer, delsektorer, størrelser og typer af enheder for økonomien og samfundet i forbindelse med cybersikkerhed. Med [...] henblik på **evalueringen** [...] tager Kommissionen højde for rapporterne fra [...] CSIRT-netværket om de erfaringer, der er gjort på [...] operationelt plan. Den første rapport forelægges senest … [54 måneder efter datoen for dette direktivs ikrafttræden].

Artikel 36

[...]

[...]

[...]

Artikel 37

Udvalgsprocedure

1. Kommissionen bistås af et udvalg. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.

2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

3. Når udvalgets udtalelse indhentes efter en skriftlig procedure, afsluttes proceduren uden noget resultat, hvis formanden for udvalget træffer beslutning herom, eller hvis et medlem af udvalget anmoder herom inden for tidsfristen for afgivelse af udtalelsen.

Artikel 38

Gennemførelse

1. **Senest** … [...]**24** måneder efter direktivets ikrafttrædelsesdato vedtager og offentliggør [...] medlemsstaterne de love og administrative bestemmelser, der er nødvendige for at efterkomme dette direktiv. De underretter straks Kommissionen herom. De anvender disse love og bestemmelser fra den ... [én dag efter den dato, der er nævnt i første afsnit].

2. Lovene og bestemmelserne skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastsættes af medlemsstaterne.

Artikel 39

Ændring af forordning (EU) nr. 910/2014

Artikel 19 [...] **i forordning (EU) nr. 910/2014** udgår **med virkning fra den ... [datoen for gennemførelsesfristen for dette direktiv].**

Artikel 40

Ændring af direktiv (EU) 2018/1972

Artikel 40 og 41 [...] **i direktiv (EU) 2018/1972** udgår **med virkning fra den ... [datoen for gennemførelsesfristen for dette direktiv].**

Artikel 41

Ophævelse

Direktiv (EU) 2016/1148 ophæves med virkning fra den [dato for direktivets gennemførelsesfrist].

Henvisninger til direktiv (EU) 2016/1148 betragtes som henvisninger til nærværende direktiv, jf. sammenligningstabellen i bilag II[...].

Artikel 42

Ikrafttræden

Dette direktiv træder i kraft på tyvendedagen efter offentliggørelsen i Den Europæiske Unions Tidende.

Artikel 43

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den […].

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*

BILAG I

SEKTORER, DELSEKTORER OG TYPER AF ENHEDER

Sektor	Delsektor	Type enhed
1. Energi	a) Elektricitet	— Elektricitetsvirksomheder som omhandlet i artikel 2, nr. 57), i Europa-Parlamentets og Rådets direktiv (EU) 2019/944, der varetager "levering" som omhandlet i artikel 2, nr. 12), i nævnte direktiv([39])
		— Distributionssystemoperatører som omhandlet i artikel 2, nr. 29), i direktiv (EU) 2019/944
		— Transmissionssystemoperatører som omhandlet i artikel 2, nr. 35), i direktiv (EU) 2019/944
		— Producenter som omhandlet i artikel 2, nr. 38), i direktiv (EU) 2019/944
		— Udpegede elektricitetsmarkedsoperatører som omhandlet i artikel 2, nr. 8), i forordning (EU) 2019/943([40])
		— Markedsdeltagere på elektricitetsmarkedet som omhandlet i artikel 2, nr. 25), i forordning (EU) 2019/943, der leverer aggregering, fleksibelt elforbrug eller energilagringstjenester som omhandlet i artikel 2, nr. 18), 20) og

---

[39] Europa-Parlamentets og Rådets direktiv (EU) 2019/944 af 5. juni 2019 om fælles regler for det indre marked for elektricitet og om ophævelse af direktiv 2012/27/EU (EUT L 158 af 14.6.2019, s. 125).

[40] Europa-Parlamentets og Rådets forordning (EU) 2019/943 om det indre marked for elektricitet (EUT L 158 af 14.6.2019, s. 54).

		59), i direktiv (EU) 2019/944
	b) Fjernvarme og fjernkøling	— Fjernvarme eller fjernkøling som omhandlet i artikel 2, nr. 19, i direktiv (EU) 2018/2001([41]) om fremme af anvendelsen af energi fra vedvarende energikilder
	c) Olie	— Olierørledningsoperatør
		— Operatører af olieproduktion, raffinaderier og behandlingsanlæg, olielagre og olietransmission
		— Centrale lagerenheder for olie som omhandlet i artikel 2, litra f), i Rådets direktiv 2009/119/EF([42])
	d) Gas	— Forsyningsvirksomheder som omhandlet i artikel 2, nr. 8), i direktiv 2009/73/EF([43])
		— Distributionssystemoperatører som omhandlet i artikel 2, nr. 6), i direktiv 2009/73/EF
		— Transmissionssystemoperatører som omhandlet i artikel 2, nr. 4), i direktiv 2009/73/EF
		— Lagersystemoperatører som omhandlet i artikel 2, nr. 10), i direktiv 2009/73/EF

---

[41] Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 af 11. december 2018 om fremme af anvendelsen af energi fra vedvarende energikilder (EUT L 328 af 21.12.2018, s. 82).

[42] Rådets direktiv 2009/119/EF af 14. september 2009 om forpligtelse for medlemsstaterne til at holde minimumslagre af råolie og/eller olieprodukter (EUT L 265 af 9.10.2009, s. 9).

[43] Europa-Parlamentets og Rådets direktiv 2009/73/EF af 13. juli 2009 om fælles regler for det indre marked for naturgas og om ophævelse af direktiv 2003/55/EF (EUT L 211 af 14.8.2009, s. 94).

		— LNG-systemoperatører som omhandlet i artikel 2, nr. 12), i direktiv 2009/73/EF
		— Naturgasvirksomheder som omhandlet i artikel 2, nr. 1), i direktiv 2009/73/EF
		— Naturgasoperatør, raffinaderier og behandlingsanlæg
	e) Brint	Operatører inden for brintproduktion, -lagring og -transmission
2. Transport	a) Luft	— Luftfartsselskaber som omhandlet i artikel 3, nr. 4), i forordning (EF) nr. 300/2008([44]), **som anvendes til kommercielle formål**
		— Lufthavnsdriftsorganer som omhandlet i artikel 2, nr. 2), i Europa-Parlamentets og Rådets direktiv 2009/12/EF([45]), lufthavne som omhandlet i artikel 2, nr. 1), i nævnte direktiv, herunder de hovedlufthavne, der er anført i afsnit 2 i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013([46]), og enheder med tilknyttede anlæg i lufthavne
		— Trafikledelses- og kontroloperatører, der udøver flyvekontroltjenester som omhandlet i artikel 2, nr. 1), i Europa-

---

[44] Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed inden for civil luftfart og om ophævelse af forordning (EF) nr. 2320/2002 (EUT L 97 af 9.4.2008, s. 72).

[45] Europa-Parlamentets og Rådets direktiv 2009/12/EF af 11. marts 2009 om lufthavnsafgifter (EUT L 70 af 14.3.2009, s. 11).

[46] Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 af 11. december 2013 om Unionens retningslinjer for udvikling af det transeuropæiske transportnet og om ophævelse af afgørelse nr. 661/2010/EU (EUT L 348 af 20.12.2013, s. 1).

		Parlamentets og Rådets forordning (EF) nr. 549/2004([47])
	b) Jernbane	— Infrastrukturforvaltere som omhandlet i artikel 3, nr. 2), i direktiv 2012/34/EU([48])
		— Jernbanevirksomheder som omhandlet i artikel 3, nr. 1), i direktiv 2012/34/EU, herunder operatører af servicefaciliteter som omhandlet i artikel 3, nr. 12), i direktiv 2012/34/EU
	c) Vand	— Rederier, som udfører passager- og godstransport ad indre vandveje, i højsøfarvand eller kystnært farvand i form af søtransport som omhandlet i bilag I til Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004([49]), bortset fra de enkelte fartøjer, som drives af disse rederier
		— Driftsorganer for havne som omhandlet i artikel 3, nr. 1), i Europa-Parlamentets og Rådets direktiv 2005/65/EF([50]), herunder deres havnefaciliteter som omhandlet i artikel 2, nr. 11), i forordning (EF) nr. 725/2004, og enheder, der driver anlæg og udstyr i havne

---

[47] Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 af 10. marts 2004 om rammerne for oprettelse af et fælles europæisk luftrum ("rammeforordningen") (EUT L 96 af 31.3.2004, s. 1).

[48] Europa-Parlamentets og Rådets direktiv 2012/34/EU af 21. november 2012 om oprettelse af et fælles europæisk jernbaneområde (EUT L 343 af 14.12.2012, s. 32).

[49] Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 af 31. marts 2004 om bedre sikring af skibe og havnefaciliteter (EUT L 129 af 29.4.2004, s. 6).

[50] Europa-Parlamentets og Rådets direktiv 2005/65/EF af 26. oktober 2005 om bedre havnesikring (EUT L 310 af 25.11.2005, s. 28).

		— Operatører af skibstrafiktjenester som omhandlet i artikel 3, litra o), i direktiv 2002/59/EF([51])
	d) Vejtransport	— Vejmyndigheder som omhandlet i artikel 2, nr. 12), i Kommissionens delegerede forordning (EU) 2015/962([52]), der er ansvarlige for trafikledelse, **med undtagelse af offentlige enheder, for hvem trafikledelse eller operatører af intelligente transportsystemer kun er en ikkevæsentlig del af deres generelle aktiviteter**
		— Operatører af intelligente transportsystemer, jf. artikel 4, nr. 1), i direktiv 2010/40/EU([53])
3. Bankvirksomhed		— Kreditinstitutter som omhandlet i artikel 4, nr. 1), i forordning (EU) nr. 575/2013 ([54]) **[med undtagelse af dem, der er omhandlet i artikel 2, stk. 5, nr. 8), i direktiv 2013/36/EU, som er fritaget i henhold til artikel 2, stk. 4, i forordning XX [DORA]]**

---

[51] Europa-Parlamentets og Rådets direktiv 2002/59/EF af 27. juni 2002 om oprettelse af et trafikovervågnings- og trafikinformationssystem for skibsfarten i Fællesskabet og om ophævelse af Rådets direktiv 93/75/EØF (EFT L 208 af 5.8.2002, s. 10).

[52] Kommissionens delegerede forordning (EU) 2015/962 af 18. december 2014 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2010/40/EU for så vidt angår tilrådighedsstillelse af EU-dækkende tidstro trafikinformationstjenester (EUT L 157 af 23.6.2015, s. 21).

[53] Europa-Parlamentets og Rådets direktiv 2010/40/EU af 7. juli 2010 om rammerne for indførelse af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportformer (EUT L 207 af 6.8.2010, s. 1).

[54] Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber og om ændring af forordning (EU) nr. 648/2012 (EUT L 176 af 27.6.2013, s. 1).

4. Finansielle markedsinfrastrukturer		— Operatører af markedspladser som omhandlet i artikel 4, nr. 24), i direktiv 2014/65/EU([55])
		— Centrale modparter (CCP) som omhandlet i artikel 2, nr. 1), i forordning (EU) nr. 648/2012([56])
5. Sundhed		— Sundhedstjenesteydere som omhandlet i artikel 3, litra g), i direktiv 2011/24/EU([57])
		— EU-referencelaboratorier som omhandlet i artikel 15 i forordning XXXX/XXXX om alvorlige grænseoverskridende sundhedstrusler([58])
		— Enheder, der udfører forsknings- og udviklingsaktiviteter vedrørende lægemidler som omhandlet i artikel 1, nr. 2), i direktiv 2001/83/EF([59]) — Enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater som omhandlet i hovedafdeling C, hovedgruppe 21, i NACE rev. 2 — Enheder, der fremstiller medicinsk udstyr, som betragtes som kritisk under en folkesundhedskrise ("listen

---

[55] Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014, s. 349).

[56] Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 201 af 27.7.2012, s. 1).

[57] Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (EUT L 88 af 4.4.2011, s. 45).

[58] [Europa-Parlamentets og Rådets forordning om alvorlige grænseoverskridende sundhedstrusler og om ophævelse af afgørelse nr. 1082/2013/EU, henvisning ajourføres, når forslaget COM(2020) 727 final er vedtaget].

[59] Europa-Parlamentets og Rådets direktiv 2001/83/EF af 6. november 2001 om oprettelse af en fællesskabskodeks for humanmedicinske lægemidler (EFT L 311 af 28.11.2001, s. 67).

		over kritisk folkesundhedsudstyr"), jf. artikel 20 i forordning XXXX([60])
6. Drikkevand		Leverandører og distributører af "drikkevand" som omhandlet i artikel 2, nr. 1), litra a), i Rådets direktiv 98/83/EF([61]), bortset fra distributører, for hvem distribution af drikkevand kun er en **ikkeväsentlig** del af deres generelle aktivitet med distribution af andre råvarer og varer [...]
7. Spildevand		Virksomheder, der indsamler, bortskaffer eller behandler byspildevand, husspildevand og industrispildevand som omhandlet i artikel 2, nr. 1)-3), i Rådets direktiv 91/271/EØF([62]), **bortset fra virksomheder, for hvem indsamling, bortskaffelse eller behandling af byspildevand, husspildevand og industrispildevand kun er en ikkeväsentlig del af deres generelle aktiviteter** [...]
8. Digital infrastruktur		— Udbydere af internetudvekslingspunkter
		— DNS-tjenesteudbydere**, bortset fra operatører af rodnavneservere**
		— Topdomænenavneadministratorer
		— Udbydere af

---

[60] [Europa-Parlamentets og Rådets forordning om styrkelse af Det Europæiske Lægemiddelagenturs rolle i forbindelse med kriseberedskab og krisestyring med hensyn til lægemidler og medicinsk udstyr, henvisning skal ajourføres, når forslaget COM(2020) 725 final er vedtaget].

[61] Rådets direktiv 98/83/EF af 3. november 1998 om kvaliteten af drikkevand (EFT L 330 af 5.12.1998, s. 32).

[62] Rådets direktiv 91/271/EØF af 21. maj 1991 om rensning af byspildevand (EFT L 135 af 30.5.1991, s. 40).

		cloudcomputingtjenester
		— Udbydere af datacentertjenester
		— Udbydere af indholdsdistributionsnetværk
		— Tillidstjenesteudbydere som omhandlet i artikel 3, nr. 19), i forordning (EU) nr. 910/2014([63])
		— Udbydere af offentlige elektroniske kommunikationsnet som omhandlet i artikel 2, nr. 8), i direktiv (EU) 2018/1972([64]) eller udbydere af elektroniske kommunikationstjenester som omhandlet i artikel 2, nr. 4), i direktiv (EU) 2018/1972, hvis deres tjenester er offentligt tilgængelige
8.a Forvaltning af IKT-tjenester **(B2B)**		**— Udbydere af administrerede tjenester** **— Udbydere af administrerede sikkerhedstjenester**

---

[63] Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

[64] Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EUT L 321 af 17.12.2018, s. 36).

9. Offentlige forvaltnings**enheder**		— Centralregeringers offentlige forvaltningsenheder **som defineret af en medlemsstat i henhold til national ret** — [...][65][...] — [...]
10. Rummet		— Operatører af jordbaseret infrastruktur, der ejes, forvaltes og drives af medlemsstater eller private parter, og som understøtter levering af rumbaserede tjenester, undtagen udbydere af offentlige elektroniske kommunikationsnet som omhandlet i artikel 2, nr. 8), i direktiv 2018/1972/EU

---

[65] [...].

BILAG II

SEKTORER, DELSEKTORER OG TYPER AF ENHEDER

Sektor	Delsektor	Type enhed
1. Post- og kurertjenester		Udbydere af posttjenester som omhandlet i artikel 2, nr. 1[...]), i direktiv 97/67/EF(66), **herunder** [...] udbydere af kurertjenester
2. Affaldshåndtering		Virksomheder, der varetager affaldshåndtering som omhandlet i artikel 3, nr. 9), i direktiv 2008/98/EF(67), men med undtagelse af virksomheder, for hvilke affaldshåndtering ikke er deres vigtigste økonomiske aktivitet

---

[66] Europa-Parlamentets og Rådets direktiv 97/67/EF af 15. december 1997 om fælles regler for udvikling af Fællesskabets indre marked for posttjenester og forbedring af disse tjenesters kvalitet (EFT L 15 af 21.1.1998, s. 14) **som ændret ved Europa-Parlamentets og Rådets direktiv 2008/6/EF af 20. februar 2008 om ændring af direktiv 97/67/EF med henblik på fuld realisering af det indre marked for posttjenester i Fællesskabet (EUT L 52 af 27.2.2008, s. 3)**.

[67] Europa-Parlamentets og Rådets direktiv 2008/98/EF af 19. november 2008 om affald og om ophævelse af visse direktiver (EUT L 312 af 22.11.2008, s. 3).

3. Fremstilling, produktion og distribution af kemikalier		Virksomheder, der beskæftiger sig med fremstilling [...] og distribution af stoffer og [...] **blandinger** som omhandlet i artikel 3, nr. [...]), 9) og 14), i forordning (EF) nr. 1907/2006(68), **og virksomheder, der ved hjælp af stoffer eller blandinger beskæftiger sig med produktion af artikler som omhandlet i nævnte forordnings artikel 3, nr. 3)**
4. Fremstilling, bearbejdning og distribution af fødevarer		Fødevarevirksomheder som omhandlet i artikel 3, nr. 2), i forordning (EF) nr. 178/2002(69)**, som beskæftiger sig med engrosforhandling og industriel produktion og tilvirkning**
5. Fremstilling	a) Fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik	Enheder, der fremstiller medicinsk udstyr som omhandlet i artikel 2, nr. 1), i forordning (EU) 2017/745(70), og enheder, der fremstiller medicinsk udstyr til in vitro-diagnostik, jf. artikel 2, nr. 2), i forordning (EU) 2017/746(71), med undtagelse af enheder, der fremstiller medicinsk udstyr, som er nævnt i bilag 1, punkt 5

---

[68] Europa-Parlamentets og Rådets forordning (EF) nr. 1907/2006 af 18. december 2006 om registrering, vurdering og godkendelse af samt begrænsninger for kemikalier (REACH), om oprettelse af et europæisk kemikalieagentur og om ændring af direktiv 1999/45/EF og ophævelse af Rådets forordning (EØF) nr. 793/93 og Kommissionens forordning (EF) nr. 1488/94 samt Rådets direktiv 76/769/EØF og Kommissionens direktiv 91/155/EØF, 93/67/EØF, 93/105/EF og 2000/21/EF (EUT L 396 af 30.12.2006, s. 1).

[69] Europa-Parlamentets og Rådets forordning (EF) nr. 178/2002 af 28. januar 2002 om generelle principper og krav i fødevarelovgivningen, om oprettelse af Den Europæiske Fødevaresikkerhedsautoritet og om procedurer vedrørende fødevaresikkerhed (EFT L 31 af 1.2.2002, s. 1).

[70] Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr, om ændring af direktiv 2001/83/EF, forordning (EF) nr. 178/2002 og forordning (EF) nr. 1223/2009 og om ophævelse af Rådets direktiv 90/385/EØF og 93/42/EØF (EUT L 117 af 5.5.2017, s. 1).

[71] Europa-Parlamentets og Rådets forordning (EU) 2017/746 af 5. april 2017 om medicinsk udstyr til in vitro-diagnostik og om ophævelse af direktiv 98/79/EF og Kommissionens afgørelse 2010/227/EU (EUT L 117 af 5.5.2017, s. 176).

	b) Fremstilling af computere og elektroniske og optiske produkter	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 26, i NACE rev. 2
	c) Fremstilling af elektrisk udstyr	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 27, i NACE rev. 2
	d) Fremstilling af maskiner og udstyr i.a.n.	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 28, i NACE rev. 2
	e) Fremstilling af motorkøretøjer, påhængsvogne og sættevogne	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 29, i NACE rev. 2
	f) Fremstilling af andre transportmidler	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 30, i NACE rev. 2
6. Digitale udbydere		— Udbydere af onlinemarkedspladser
		— Udbydere af onlinesøgemaskiner
		— Udbydere af sociale netværkstjenester